الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T X.1521

(2016/03)

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل مواطن الضعف/الحالة

## نظام تحديد درجات لمواطن الضعف الشائعة 3.0

التوصية ITU-T X.1521

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

| | |
|---|---|
| الشبكات العمومية للبيانات | X.199–X.1 |
| التوصيل البيني للأنظمة المفتوحة | X.299–X.200 |
| التشغيل البيني للشبكات | X.399–X.300 |
| أنظمة معالجة الرسائل | X.499–X.400 |
| الدليل | X.599–X.500 |
| التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام | X.699–X.600 |
| إدارة التوصيل البيني للأنظمة المفتوحة (OSI) | X.799–X.700 |
| الأمن | X.849–X.800 |
| تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI) | X.899–X.850 |
| المعالجة الموزعة المفتوحة | X.999–X.900 |
| آمن المعلومات والشبكات | |
| الجوانب العامة للأمن | X.1029–X.1000 |
| أمن الشبكة | X.1049–X.1030 |
| إدارة الأمن | X.1069–X.1050 |
| القياسات البيومترية عن بُعد | X.1099–X.1080 |
| تطبيقات وخدمات آمنة | |
| أمن البث المتعدد | X.1109–X.1100 |
| أمن الشبكة المحلية | X.1119–X.1110 |
| أمن الخدمات المتنقلة | X.1139–X.1120 |
| أمن الويب | X.1149–X.1140 |
| بروتوكولات الأمن | X.1159–X.1150 |
| الأمن بين جهتين نظيرتين | X.1169–X.1160 |
| أمن معرفات الهوية عبر الشبكات | X.1179–X.1170 |
| أمن التلفزيون القائم على بروتوكول الإنترنت | X.1199–X.1180 |
| آمن الفضاء السيبراني | |
| الأمن السيبراني | X.1229–X.1200 |
| مكافحة الرسائل الاقتحامية | X.1249–X.1230 |
| إدارة الهوية | X.1279–X.1250 |
| تطبيقات وخدمات آمنة | |
| اتصالات الطوارئ | X.1309-X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1339–X.1310 |
| التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية | X.1349–X.1340 |
| تبادل معلومات الأمن السيبراني | |
| نظرة عامة عن الأمن السيبراني | X.1519–X.1500 |
| **تبادل مواطن الضعف/الحالة** | **X.1539–X.1520** |
| تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية | X.1549–X.1540 |
| تبادل السياسات | X.1559–X.1550 |
| طلب المعلومات الحدسية والمعلومات الأخرى | X.1569–X.1560 |
| تعرف الهوية والاكتشاف | X.1579–X.1570 |
| التبادل المضمون | X.1589–X.1580 |
| آمن الحوسبة السحابية | |
| نظرة عامة على أمن الحوسبة السحابية | X.1601–X.1600 |
| تصميم أمن الحوسبة السحابية | X.1639–X.1602 |
| أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية | X.1659–X.1640 |
| تنفيذ أمن الحوسبة السحابية | X.1679–X.1660 |
| أمن أشكال أخرى للحوسبة السحابية | X.1699–X.1680 |

*لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.*

**التوصية ITU-T X.1521**

# نظام تحديد درجات لمواطن الضعف الشائعة 3.0


## ملخص

توفر هذه التوصية المعنية بنظام تحديد درجات لمواطن الضعف الشائعة (CVSS) إطاراً مفتوحاً للتعبير عن خصائص وتأثيرات مواطن ضعف تكنولوجيا المعلومات والاتصالات في برمجيات المصدر المفتوح أو البرمجيات التجارية المستخدمة في شبكات الاتصالات أو أجهزة المستخدم النهائي أو أي من الأنواع الأخرى لتكنولوجيا المعلومات والاتصالات القادرة على تشغيل البرمجيات. والهدف من التوصية هو تمكين مديري تكنولوجيا المعلومات والاتصالات وموردي النشرات المعنية بالثغرات الأمنية وباعة الأمن وباعة التطبيقات والباحثين من التخاطب بلغة مشتركة بشأن نظام تحديد درجات لمواطن الضعف في تكنولوجيا المعلومات والاتصالات.



## التسلسل التاريخي

| الصيغة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1521 | 2011/04/20 | 17 | 11.1002/1000/11062 |
| 2.0 | ITU-T X.1521 | 2016/03/23 | 17 | 11.1002/1000/12614 |


## مصطلحات أساسية

نظام تحديد درجات لمواطن الضعف الشائعة (CVSS)، تبادل معلومات الأمن السيبراني (CYBEX)، مقاييس

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بمعرّف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

## تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

## ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

## حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

# جدول المحتويات

**الصفحة**

**مقدمة**

يُشكل نظام تحديد درجات لمواطن الضعف الشائعة (CVSS) إطاراً مفتوحاً للتعبير عن خصائص مواطن الضعف في البرمجيات وعن حدّة مواطن الضعف هذه. ويتألف نظام تحديد درجات لمواطن الضعف الشائعة من ثلاث فئات من المقاييس هي: المقاييس القاعدية والمقاييس الزمنية والمقاييس البيئية. وتمثل الفئة القاعدية السمات المتأصلة لموطن الضعف، وتعكس الفئة الزمنية خصائص موطن الضعف المتغيرة مع الزمن، وتمثل الفئة البيئية خصائص موطن الضعف التي تنفرد بها بيئة المستخدم. وتنتج المقاييس القاعدية علامة تتراوح من صفر إلى 10 ويمكن أن تتغير هذه العلامة بناء على علامات المقاييس الزمنية والبيئية. وتمثَّل أيضاً علامة نظام تحديد درجات لمواطن الضعف الشائعة CVSS في شكل سلسلة متجهات وتمثيل نصي مضغوط يعكس القيم المستعملة لإنتاج العلامة. وتعرض هذه التوصية المواصفات الرسمية للإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

ويتضمن الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة تحسينات كبيرة مقارنة بالإصدار 2.0 وهو غير متوافق رجعياً معه. فأثناء استخدام الإصدار 2.0، تبيّن أن مواصفات هذا الإصدار تشكو من عدة أوجه قصور ومن بينها ما يلي: وضع علامة لمواطن الضعف في بيئة افتراضية، وتمثيل مواطن الضعف "غير المباشرة" مثل البرمجة العابرة للموقع، وعدم القدرة على استخلاص أوجه الترابط بين التطبيقات في النظام الواحد، والتقاط أعمال المستخدمين من غير المهاجمين. وتتضّمن الفقرة 2 من التذييل I معلومات إضافية عن التحسينات المدخلة في الإصدار 3.0.

وفيما كان يسعى فريق العمل المعني بنظام تحديد درجات لمواطن الضعف الشائعة إلى معالجة أوجه القصور هذه، أدرك أنه لن يتمكّن من الحفاظ على توافق رجعي مع الإصدار 2.0. وإذ نقرّ بأن انعدام التوافق هذا سيسبّب بعض المشاكل في الأنظمة القائمة التي تستخدم الإصدار 2.0 وتقوم بمعالجته، نعتقد أن القيمة المضافة التي يقدّمها الإصدار 3.0 ستكون كافية للتعويض عن هذا الإزعاج. وننصح بشدّة المستخدمين والبائعين الذين ينتجون اليوم الإصدار 2.0 ويقومون بمعالجته بالانتقال إلى الإصدار 3.0.

وستبقى مواصفة الإصدار 2.0 متاحاً لأغراض تاريخية ولكنها لن يكون فاعلة. ويُدعى المعنيون بتنفيذ الأدوات والعمليات بشدة إلى اعتماد مواصفة الإصدار 3.0 مع مواصلة دعم الإصدار 2.0 بغية معالجة مواطن الضعف التي نُسبت لها علامة بالفعل في مواصفة الإصدار 2.0.

# نظام تحديد درجات لمواطن الضعف الشائعة 0.3

## 1 مجال التطبيق

تقدم هذه التوصية نهجاً موحداً للتعبير عن خصائص وتأثيرات مواطن ضعف تكنولوجيا المعلومات والاتصالات باستخدام مقاييس زمنية وبيئية تطبق معلومات سياقية كي تعكس بمزيد من الدقة مخاطر البيئة الفريدة لكل مستخدم.

وتُعتبر هذه التوصية من الناحية التقنية متكافئة ومتوافقة مع "الإصدار الثالث من نظام تحديد درجات لمواطن الضعف الشائعة (CVSS)"، الصادر بتاريخ 10 يونيو 2015، والذي يمكن الاطلاع عليه في الموقع الإلكتروني التالي: http://www.first.org/cvss.

## 2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل، من خلال الإشارة إليها في هذا النص، جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع مستخدمي هذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا يوجد.

## 3 التعاريف

### 1.3 مصطلحات معرفة في أماكن أخرى

تستخدم هذه التوصية المصطلح التالي المعرّف في مكان آخر:

**1.1.3 موطن الضعف** [b-ITU-T X.1500]: أي مواطن ضعف يمكن استغلالها لانتهاك نظام أو المعلومات التي يحتوي عليها.

### 2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

**1.2.3 النفاذ**: قدرة طرف فاعل على رؤية طرف مفعول به وتعديله والتواصل معه. ويتيح النفاذ تدفق المعلومات بين هذين الطرفين.

**2.2.3 التيسّر**: موثوقية الأفراد المخولين ونفاذهم في الوقت المناسب إلى البيانات والموارد.

**3.2.3 السرية**: مبدأ أمني يعمل على ضمان عدم الإفصاح عن معلومات لأطراف فاعلة غير مخولة.

**4.2.3 الحصانة**: مبدأ أمني يضمن عدم تعديل المعلومات والأنظمة بسوء نية أو عرضاً.

**5.2.3 الخطر**: التأثير النسبي لموطن ضعف مُستغَل على بيئة المستخدم.

**6.2.3 التهديد**: احتمال أو تواتر وقوع حدث ضار.

## 4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

A التأثير على التيسُّر *(Availability Impact)*

AC تعقيد الهجوم *(Attack Complexity)*

AR متطلب التيسر *(Availability Requirement)*

ARP بروتوكول استبانة العنوان *(Address Resolution Protocol)*

AV متجه الهجوم *(Attack Vector)*

C التأثير على السرية *(Confidentiality Impact)*

CIA السرية والحصانة والتيسر *(Confidentiality, Integrity, and Availability)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CR متطلب السرية *(Confidentiality Requirement)*

CVE موطِن الضعف والتعرّض الشائع *(Common Vulnerability Exposure)*

CVSS نظام تحديد درجات لمواطن الضعف الشائعة *(Common Vulnerability Scoring System)*

CWE تعداد مواطن الضعف الشائعة *(Common Weakness Enumeration)*

DMA النفاذ المباشر إلى الذاكرة *(Direct Memory Access)*

DNS نظام أسماء الميادين *(Domain Name System)*

DOM نموذج موضوع وثائقي *(Document Object Model)*

DoS الحرمان من الخدمة *(Denial-of-Service)*

E نضج شفرة الاستغلال *(Exploit code maturity)*

I التأثير على الحصانة *(Integrity impact)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technologies)*

ID المعرف *(Identifier)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IR متطلب الحصانة *(Integrity Requirement)*

ISC العلامة الفرعية للتأثير *(Impact Sub Score)*

IT تكنولوجيا المعلومات *(Information Technology)*

LAN شبكة المنطقة المحلية *(Local Area Network)*

MA التيسّر المعدَّل *(Modified Availability)*

MAC تعقيد الهجوم المعدَّل *(Modified Attack Complexity)*

MAV متجه الهجوم المعدّل *(Modified Attack Vector)*

MC التأثير على السرية المعدَّل *(Modified Confidentiality impact)*

MI الحصانة المعدَّلة *(Modified Integrity)*

MPR الامتيازات المطلوبة المعدَّلة *(Modified Privileges Required)*

MS النطاق المعدّل *(Modified Scope)*

MUI تفاعل المستخدم المعدّل *(Modified User Interaction)*

NIST المعهد الوطني للمعايير *(National Institute of Standards)*

OS نظام التشغيل *(Operating System)*

OSI التوصيل البيني للأنظمة المفتوحة *(Open Systems Interconnection)*

PCI DSS معيار أمن بيانات قطاع بطاقات الدفع *(Payment Card Industry Data Security Standard)*

PR الامتيازات المطلوبة *(Privileges Required)*

RC الثقة في التقرير *(Report Confidence)*

RL مستوى التدارك *(Remediation Level)*

RPC نداء الإجراء عن بُعد *(Remote Procedure Call)*

S النطاق *(Scope)*

SCAP بروتوكول أتمتة المحتوى الأمني *(Security Content Automation Protocol)*

SQL لغة الاستعلام البِنْيَوية *(Structured Query Language)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

UI تفاعل المستخدم *(User Interaction)*

USB الناقل التسلسلي العام *(Universal Serial Bus)*

VM الآلة الافتراضية *(Virtual Machine)*

XSS البرمجة العابرة للموقع *(Cross Site Scripting)*

## 5 اصطلاحات

لا يوجد.

## 6 نظام تحديد درجات لمواطن الضعف الشائعة

يُشكل نظام تحديد درجات لمواطن الضعف الشائعة إطاراً مفتوحاً للتعبير عن خصائص مواطن الضعف في البرمجيات وعن حدة مواطن الضعف هذه. ويتألف نظام تحديد درجات لمواطن الضعف الشائعة من ثلاث فئات من المقاييس هي: المقاييس القاعدية والمقاييس الزمنية والمقاييس البيئية. وتمثل الفئة القاعدية السمات المتأصلة لموطن الضعف، وتعكس الفئة الزمنية خصائص موطن الضعف المتغيرة مع الزمن، وتمثل الفئة البيئية خصائص موطن الضعف التي تنفرد بها بيئة المستخدم. وتنتج المقاييس القاعدية علامة تتراوح من صفر إلى 10 ويمكن أن تتغير هذه العلامة بناءً على علامات المقاييس الزمنية والبيئية. وتمثَّل أيضاً علامة نظام تحديد درجات لمواطن الضعف الشائعة في شكل سلسلة متجهات وتمثيل نصي مضغوط يعكس القيم المستعملة لإنتاج العلامة. وتعرض هذه التوصية المواصفات الرسمية للإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

## 1.6 مقدمة

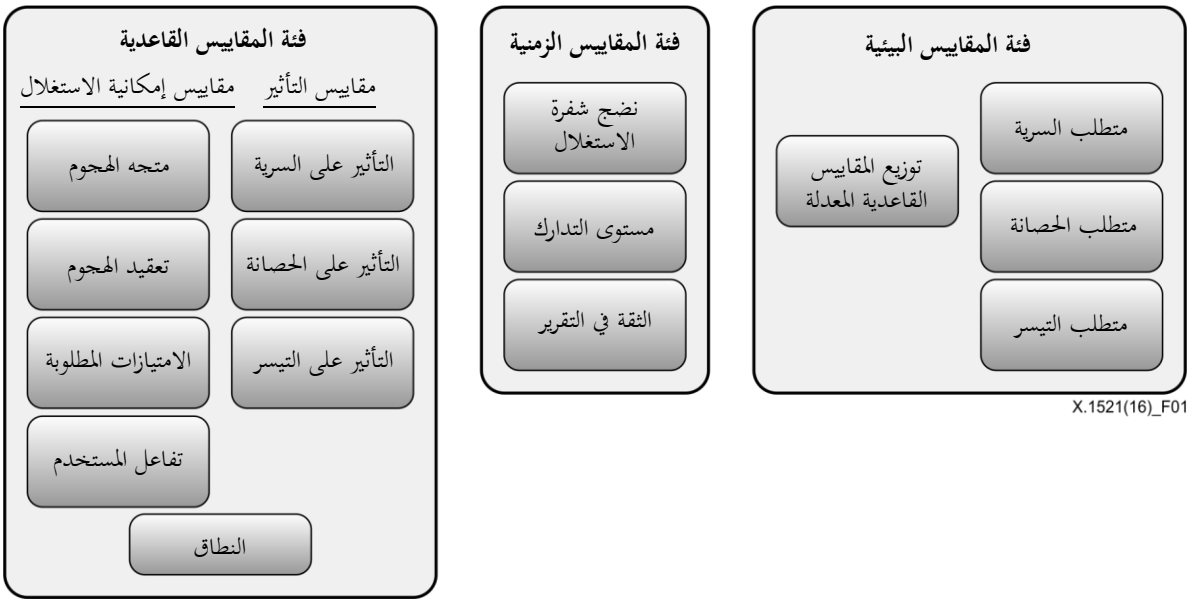
تشكّل مواطن الضعف في البرمجيات، والمعدات الحاسوبية، والبرامج الحاسوبية الثابتة خطراً حرجاً على أي منظمة تدير شبكة حاسوبية، ويصعب تصنيف مواطن الضعف هذه والتخفيف من ضررها. ويتضمّن نظام تحديد درجات لمواطن الضعف الشائعة طريقة لاستخلاص الخصائص الرئيسية لموطن الضعف وإنتاج علامةٍ رقمية تبيّن حدّة موطن الضعف هذا وتمثيلٍ نصي عن هذه العلامة. ويمكن بعد ذلك ترجمة هذه العلامة الرقمية إلى تمثيل نوعي (يحدد مثلاً ما إذا كان المستوى منخفضاً أو متوسطاً أو عالياً أو حرجاً) بغية مساعدة المنظمات على إجراء تقييم صائب للعمليات التي تتبعها لإدارة مواطن الضعف وعلى ترتيبها بحسب الأولوية.

وباختصار، يوفّر نظام تحديد درجات لمواطن الضعف الشائعة ثلاث منافع مهمة. ويتيح أولاً وضع علامات موحدة لمواطن الضعف. فعندما تستعمل منظمة خوارزمية مشتركة لوضع علامات لمواطن الضعف التي تشوب جميع منصات تكنولوجيا المعلومات، يمكنها الاستفادة من سياسة واحدة لإدارة مواطن الضعف تحدد المهلة القصوى الممنوحة للتأكد من وجود موطن ضعف معيّن وإصلاحه. وثانياً، يوفّر هذا النظام إطاراً مفتوحاً. فقد يختلط الأمر على المستخدم عندما يسند طرف ثالث علامة اعتباطية لموطن ضعف. وعند استخدام نظام تحديد درجات لمواطن الضعف الشائعة، تكون الخصائص الفردية المستخدمة لاستخلاص العلامة متسمة بالشفافية. وأخيراً، يتيح النظام ترتيب أولويات المخاطر. فعند حساب العلامة البيئية، يصبح موطن الضعف سياقياً لكل منظمة، ويساعد على تحسين فهم الخطر الذي تتعرض له المنظمة نتيجة موطن الضعف هذا.

وتصف هذه التوصية المواصفات الرسمية للإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

### 1.1.6 المقاييس

يتألف نظام تحديد درجات لمواطن الضعف الشائعة من ثلاث فئات مقاييس، وهي المقاييس القاعدية والزمنية والبيئية، ويتألف كل منها من مجموعة من المقاييس، على النحو المبين في الشكل 1.




**الشكل 1 – فئات مقاييس الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة**

تمثل فئة المقاييس القاعدية الخصائص الجوهرية لموطن الضعف فتكون ثابتة على مر الزمن وعبر بيئات المستخدم. وتتألف هذه الفئة من مجموعتين من المقاييس هما: مقاييس إمكانية الاستغلال ومقاييس التأثير.

أما مقاييس إمكانية الاستغلال فتبيّن مدى سهولة استغلال موطن الضعف والوسائل التقنية التي تسمح بذلك. وبالتالي، فهي تمثّل خصائص *الشيء المتسم بالضعف* وهو ما يطلق عليه رسمياً تسمية *المكوّن الضعيف*. وأما مقاييس التأثير فتبيّن الآثار الناجمة عن استغلال ناجح وتمثل الآثار الواقعة على *الشيء الذي تعرض للتأثير* والذي يطلق عليه رسمياً تسمية *المكون المتأثر*.

ويكون المكوّن الضعيف عادة تطبيقاً برمجياً أو وحدة برمجية أو برنامج تشغيل أو غير ذلك (أو حتى إحدى المعدات الحاسوبية)، بينما يمكن أن يكون المكوّن المتأثر تطبيقاً برمجياً أو معدة حاسوبية أو مورداً شبكياً. وتُعتبر هذه القدرة على قياس أثر موطن ضعف غير المكوّن الضعيف أحد السمات الرئيسية للإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة. ويتم تناول هذه الخاصية والتمعن في بحثها في إطار مقياس النطاق أدناه.

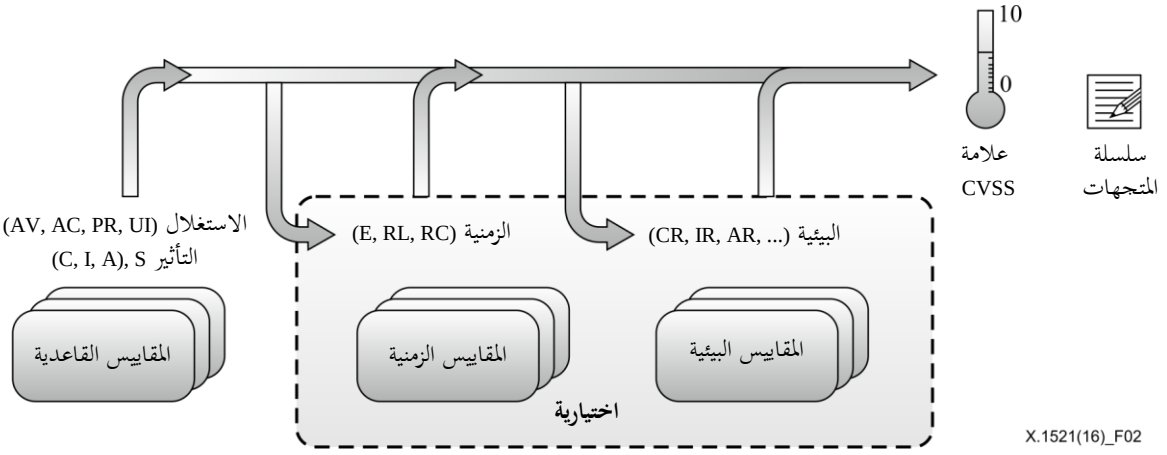
وتعكس فئة المقاييس الزمنية خصائص موطن الضعف الذي قد يتغير بمرور الوقت ولكن ليس عبر بيئات المستخدم. وعلى سبيل المثال، يؤدي وجود حزمة استغلال سهلة الاستخدام إلى زيادة علامة نظام تحديد الدرجات لمواطن الضعف الشائعة، في حين أن إيجاد حل رسمي يؤدي إلى خفضها.

وتمثل فئة المقاييس البيئية خصائص موطن الضعف المرتبطة بالبيئة الخاصة بالمستخدم والتي تنفرد بها هذه البيئة. وتسمح هذه المقاييس للمحلل المعني بوضع العلامات بإدماج ضوابط أمنية يمكن أن تخفف من أي آثار قد تحدث وأن تزيد أو تخفف من أهمية النظام الضعيف بحسب مخاطره التجارية.

ويتم فيما يلي بحث كل من هذه المقاييس بمزيد من التفاصيل.

### 2.1.6 تحديد العلامة

عندما يسند المحلل قيماً إلى المقاييس القاعدية، تحسب المعادلة القاعدية علامة تتراوح بين 0.0 و10.0 على النحو المبين في الشكل 2.




**الشكل 2 – مقاييس ومعادلات نظام تحديد درجات لمواطن الضعف الشائعة**

وبصفة خاصة، تشتق المعادلة القاعدية من معادلتين فرعيتين هما: معادلة العلامة الفرعية لإمكانية الاستغلال ومعادلة العلامة الفرعية للتأثير. وتنتج معادلة العلامة الفرعية لإمكانية الاستغلال عن المقاييس القاعدية لإمكانية الاستغلال في حين تنتج معادلة العلامة الفرعية للتأثير عن المقاييس القاعدية للتأثير.

ويمكن عندئذ تعزيز دقة العلامة القاعدية بوضع علامة للمقاييس الزمنية والبيئية من أجل إلقاء الضوء، بمزيد من الدقة، على الخطر الذي يشكله موطن ضعف على بيئة المستخدم. ومع ذلك، فإن وضع علامة للمقاييس الزمنية والبيئية ليس إلزامياً.

وبصفة عامة، يقوم محللو نشرة الثغرات الأمنية أو باعة المنتجات الأمنية أو باعة التطبيقات بتوصيف المقياسين القاعدي والزمني لأنهم يملكون عادة معلومات أدق عن خصائص مواطن الضعف من المستخدمين. ومن جهة أخرى، توصّف منظمات المستعملين النهائيين المقاييس البيئية لأنها الأقدر على تقييم الأثر المحتمل لموطن ضعف ضمن بيئة الحوسبة الخاصة بها.

كما أن وضع علامة لمقاييس نظام تحديد الدرجات لمواطن الضعف الشائعة ينتج سلسلة متجهات وتمثيلاً نصياً لقيم المقاييس المستخدمة لتحديد علامة موطن الضعف. وسلسلة المتجهات هذه هي سلسلة نصية لها نسق معيّن تتضمن جميع القيم المسندة إلى كل من المقاييس، وينبغي عرضها دائماً مع علامة موطن الضعف.

ويرد فيما يلي شرح لمعادلات حساب العلامات ولسلسلة المتجهات.

وجدير بالذكر أن علامات جميع المقاييس ينبغي أن توضع مع افتراض أن المهاجم تعرّف بالفعل على موطن الضعف وقام بتحديده. ومن هنا، لا يحتاج المحلل إلى النظر في الطريقة التي حُدد بها موطن الضعف. وبالإضافة إلى ذلك، يُرجح أن تقوم فئات متعددة جداً من الأطراف بتحديد علامة موطن الضعف (مثل باعة البرمجيات، ومحللي نشرة الثغرات الأمنية، وباعة المنتجات الأمنية، وغيرهم)، ولكن الجدير بالذكر أن العلامة الممنوحة لموطن الضعف ينبغي ألا تتأثر بالأطراف ومنظماتها.

## 2.6 المقاييس القاعدية

### 1.2.6 مقاييس إمكانية الاستغلال

كما ذُكر أعلاه، تعكس مقاييس إمكانية الاستغلال خصائص *الشيء* الضعيف الذي يُشار إليه رسمياً باسم *المكون الضعيف*. وبالتالي، ينبغي أن تكون علامة كل من هذه المقاييس المحددة أدناه مرتبطة بالمكون الضعيف وأن تعكس هذه المقاييسُ خصائص موطن الضعف التي تقود إلى نجاح الهجوم.

#### 1.1.2.6 متجه الهجوم (AV)

يعكس هذا المقياس السياق الذي يسمح باستغلال موطن الضعف. وتزداد قيمة هذا المقياس (وبالتالي العلامة القاعدية) كلما كان المهاجم بعيداً (من منظور المسافة المنطقية والمادية) لاستغلال المكون الضعيف. ويقوم ذلك على افتراض مفاده أن عدد المهاجمين المحتملين لمواطن الضعف التي يمكن استغلالها عبر الإنترنت هو أعلى من عدد المهاجمين المحتملين الذين يمكنهم استغلال موطن ضعف يتطلب نفاذ الفرد شخصياً إلى الجهاز المعني، ويؤدي ذلك إلى ارتفاع العلامة. وترد في الجدول 1 قائمة بالقيم الممكنة.

**الجدول 1 – متجه الهجوم**

| قيمة المقياس | الشرح |
|---|---|
| شبكة (N) | موطن الضعف الذي يمكن استغلاله بالنفاذ إلى الشبكة يعني أن المكون الضعيف مسند إلى كدسة الشبكة وأن مسار المهاجم مرّ عبر الطبقة 3 من التوصيل البيني للأنظمة المفتوحة (OSI) (طبقة الشبكة). وكثيراً ما يوصف موطن الضعف هذا بالقول إنه "قابل للاستغلال عن بُعد" ويمكن أن يُعتبر هجوماً يجوز استغلاله على بعد قفزة شبكية أو أكثر (مثلاً من مسيرات عبر حدود الطبقة 3). ومن الأمثلة على هجوم الشبكة مهاجم يتسبب بحرمان من الخدمة (DoS) من خلال إرسال حزمة مبتكرة لبروتوكول التحكّم في الإرسال (TCP) بواسطة الإنترنت العمومي (مثل CVE-2004-0230). |
| شبكة مجاورة (A) | موطن الضعف الذي يمكن استغلاله بالنفاذ إلى شبكة مجاورة يعني أن المكون الضعيف مسند إلى كدسة الشبكة، إلا أن الهجوم يقتصر على نفس الشبكة المادية (مثل بلوتوث وIEEE 802.11) أو المنطقية (مثل شبكة بروتوكول الإنترنت الفرعية المحلية) المشتركة ولا يمكن أن يتمّ هذا الهجوم عن طريق حدود الطبقة 3 من التوصيل البيني للأنظمة المفتوحة (مثل ميسر). ومن الأمثلة على هجوم مجاور فيضانات بروتوكول استبانة العنوان (ARP) (الإصدار الرابع لبروتوكول الإنترنت (IPv4)) أو اكتشاف الجار (الإصدار السادس لبروتوكول الإنترنت (IPv6)) بما يؤدي إلى حرمان من الخدمة في إطار شبكات المنطقة المحلية (LAN). وانظر أيضاً CVE-2013-6014. |
| محلية (L) | موطن الضعف الذي يمكن استغلاله بالنفاذ محلياً يعني أن المكون الضعيف مسند إلى كدسة الشبكة وأن مسار المهاجم يمرّ عبر قدرات القراءة والكتابة والتنفيذ. وفي بعض الأحيان، قد يقوم المهاجم بالدخول محلياً من أجل استغلال موطن الضعف، أو قد يعتمد على تفاعل المستخدم (UI) لتنفيذ ملف ضارّ. |
| مادية (P) | موطن الضعف الذي يمكن استغلاله بالنفاذ مادياً يقتضي أن يتمكن المهاجم من ملامسة المكون الهش أو تحريكه مادياً. ويمكن أن يكون التفاعل المادي قصيراً (مثل هجوم الخادمة الشريرة[1]) أو متواصلاً. ومن الأمثلة على هذا النوع من الهجوم هجوم التشغيل على البارد الذي يتيح لمهاجم الحصول على مفتاح تشفير قرص بعد التمكن من النفاذ مادياً إلى النظام، أو هجمات طرفية مثل هجوم عبر Firewire/النفاذ المباشر إلى الذاكرة بواسطة الناقل التسلسلي الشامل (USB). |

[1] انظر https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html للاطلاع على وصف هجوم الخادمة الشريرة.

### 2.1.2.6 تعقيد الهجوم (AC)

يصف هذا المقياس الظروف الخارجة عن سيطرة المهاجم والتي يجب أن تكون متوافرة لاستغلال موطن الضعف. وعلى النحو الموضح أدناه، قد تتطلب هذه الظروف جمع المزيد من المعلومات بشأن الهدف أو بشأن وجود أوضاع خاصة بتشكيلة النظام أو استثناءات حاسوبية. والأهم من ذلك، لا يتضمن تقييم هذا المقياس أي متطلبات تقتضي تفاعل المستخدم من أجل استغلال موطن الضعف (وتستخلص هذه الظروف في مقياس تفاعل المستخدم). وترتفع قيمة هذا المقياس كلما قلّ تعقيد الهجوم. وترد في الجدول 2 قائمة بالقيم الممكنة.

**الجدول 2 – تعقيد الهجوم**

| قيمة المقياس | الشرح |
|---|---|
| منخفضة (L) | لا توجد شروط متخصصة للنفاذ أو ظروف مخففة. فيمكن أن يتوقع المهاجم تحقيق هجمات مكررة ناجحة على المكون الضعيف. |
| عالية (H) | يتوقف الهجوم الناجح على ظروف تخرج عن سيطرة المهاجم. وبالتالي، لا يمكن أن يحقق المهاجم هجوماً ناجحاً كلّما شاء ذلك، فعليه أن يبذل قدراً كبيراً من الجهود للتحضير للهجوم وشنه ضد المكون الضعيف قبل أن يأمل في تحقيق هجوم ناجح[2]. وعلى سبيل المثال، قد يتوقف نجاح الهجوم على قدرة المهاجم على التغلب على أحد الظروف التالية:<br>• على المهاجم أن يجري عمليات استطلاع عن المكون المستهدف، وذلك مثلاً بشأن أوضاع تشكيلة الهدف وأرقام التتابع والأسرار المشتركة وغير ذلك.<br>• على المهاجم أن يهيّئ بيئة الهدف لتحسين موثوقية الاستغلال، مثل الاستغلال المكرر للفوز بظرف تسابقي أو التغلب على التقنيات المتقدمة للتخفيف من الاستغلال.<br>• على المهاجم أن يُقحم نفسه في المسار المنطقي للشبكة بين الهدف والمورد الذي تطلبه الضحية من أجل قراءة و/أو تعديل اتصالات الشبكة (مثل هجمات الاعتراض الوسيط). |

### 3.1.2.6 الامتيازات المطلوبة (PR)

يصف هذا المقياس مستوى الامتيازات التي يجب أن يتمتع بها المهاجم *قبل* أن ينجح في استغلال موطن الضعف. وترتفع قيمة هذا المقياس عندما لا يتطلب الأمر أي امتياز. وترد في الجدول 3 قائمة بالقيم الممكنة.

**الجدول 3 – الامتيازات المطلوبة**

| قيمة المقياس | الشرح |
|---|---|
| معدومة (N) | المهاجم ليس مخولاً قبل الهجوم، وبالتالي لا يحتاج إلى الدخول إلى معلمات الضبط أو ملفات للقيام بالهجوم. |
| منخفضة (L) | المهاجم مخوّل ويتمتع بامتيازات (أي يحتاج إليها) تمنح المستخدم قدرات أساسية لا يمكن أن تؤثر عادة إلا على معلمات الضبط والملفات التي يملكها المستخدم. وإلا فقد يكون للمهاجم الذي يتمتع بامتيازات منخفضة القدرة على إحداث أثر على موارد غير حساسة فقط. |
| مرتفعة (H) | المهاجم مخول ويتمتع بامتيازات (أي يحتاج إليها) تمنح قدرة كبيرة على التحكم (الإداري مثلاً) بالمكون الضعيف مما قد يؤثر على معلمات الضبط والملفات في المكون برمته. |

[2] يُرجى ملاحظة أننا لا نبدي أي تعليق على حجم الجهود اللازمة. فنعتبر ببساطة أنه ينبغي بذل بعض الجهد الإضافي لاستغلال موطن الضعف.

### 4.1.2.6 تفاعل المستخدم (UI)

يستخلص هذا المقياس المتطلبات اللازمة ليتمكن مستخدم، غير مهاجم، من المشاركة في تعطيل المكون الضعيف بنجاح. فيحدد هذا المقياس ما إذا كان المهاجم قادراً على استغلال موطن الضعف حسب مشيئته حصراً أو ما إذا كان الأمر يستلزم مشاركة مستخدم مستقل (أو عملية يبدأها مستخدم) بشكل أو بآخر. وترتفع قيمة المقياس إلى أقصى حد لها عندما تنعدم الحاجة إلى تفاعل المستخدم. وترد في الجدول 4 قائمة بالقيم الممكنة.

**الجدول 4 – تفاعل المستخدم**

| قيمة المقياس | الشرح |
|---|---|
| معدومة (N) | يمكن استغلال النظام الضعيف دون التفاعل مع أي مستخدم. |
| ضرورية (R) | يتطلب الاستغلال الناجح لموطن الضعف هذا أن يقوم المستخدم بفعلٍ ما قبل أن يصبح استغلال موطن الضعف ممكناً. وعلى سبيل المثال، قد يكون الاستغلال الناجح ممكناً فقط أثناء قيام مسؤول النظام بتثبيت تطبيق ما. |

### 2.2.6 النطاق (S)

من الخصائص المهمة التي يستخلصها الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة إمكانية تأثير موطن ضعف يعتري مكون برمجية على موارد خارجة عن وسائلها أو امتيازاتها. وهذه التبعة يمثلها مقياس نطاق التخويل أو فقط النطاق.

ويشير النطاق رسمياً إلى مجموعة الامتيازات التي تحددها سلطة حاسوبية (مثل تطبيق أو نظام تشغيل أو بيئة افتراضية) عند منح التخويل بالنفاذ إلى الموارد الحاسوبية (مثل الملفات، ووحدة المعالجة المركزية، والذاكرة، وغير ذلك). وتُمنح هذه الامتيازات بالاعتماد على إحدى وسائل التأكد من هوية المستخدم وتخويله. وفي بعض الحالات، قد يكون التخويل بسيطاً أو مضبوطاً بصورة طفيفة بناء على قواعد أو معايير محددة مسبقاً. وعلى سبيل المثال، وفي حالة الحركة في الإثرنت المرسلة إلى بدالة شبكة، تقبل البدالة الحركة الآتية على منافذها وتصبح سلطة تتحكم بتدفق الحركة على منافذ بدالة أخرى.

وعندما يكون موطن الضعف الموجود في مكون برمجية محكوم بنطاق تخويل قادراً على التأثير على موارد يحكمها نطاق تخويل آخر، فهذا يعني أن ثمة تغيير طرأ على النطاق.

وقد يظن المرء بالفطرة أن تغير النطاق ينبع من جهاز افتراضي، ومثال على ذلك موطن ضعف يعتري آلة افتراضية تسمح للمهاجم بحذف ملفات من نظام التشغيل المضيف (OS) (ربما حتى الآلة الافتراضية (VM) الخاصة به). وفي هذا المثال، هناك سلطتا تخويل منفصلتان: الأولى تقوم بتحديد وإنفاذ الامتيازات من أجل الآلة الافتراضية ومستخدميها، والأخرى تقوم بتحديد وإنفاذ الامتيازات من أجل النظام المضيف حيث تعمل الآلة الافتراضية.

ولا يحدث مثلاً تغيير في النطاق عندما يتعلق الأمر بموطن ضعف في "مايكروسوفت وورد" يسمح لمهاجم بالنيل من جميع ملفات نظام التشغيل لأن الهيئة ذاتها تقوم بإنفاذ امتيازات نموذج "وورد" الذي يملكه المستخدم وملفات النظام المضيف.

وترتفع العلامة القاعدية عندما يطرأ تغيير في النطاق. وترد في الجدول 5 قائمة بالقيم الممكنة.

**الجدول 5 – النطاق**

| قيمة المقياس | الشرح |
|---|---|
| ثابتة (U) | لا يؤثر موطن الضعف المستغَل إلا على الموارد التي تديرها السلطة ذاتها. وفي هذه الحالة، فإن المكون الضعيف هو نفسه المكون المتأثر. |
| متغيرة (C) | يؤثر موطن الضعف المستغَل على موارد تتخطى امتيازات التخويل التي يقتضيها المكون الضعيف. وفي هذه الحالة، يختلف المكون الضعيف عن المكون المتأثر. |

### 3.2.6 مقاييس التأثير

تبيّن مقاييس التأثير خصائص المكون المتأثر. وسواء كان موطن الضعف المستغَل بنجاح يؤثر على مكون واحد أو أكثر، تحسب علامات مقاييس التأثير بالاعتماد على المكون الذي تعرض لأسوأ نتيجة ناجمة بصورة مباشرة ومتوقعة عن هجوم ناجح. ومن هنا، ينبغي للمحللين حصر التأثير بالنتيجة النهائية المعقولة التي سيتمكن المهاجم حتماً من تحقيقها في رأيهم.

وإذا لم يطرأ أي تغيير في النطاق، ينبغي لمقاييس التأثير أن تعكس التأثير على سرية وحصانة وتيسر (CIA) المكون الضعيف. أما إذا طرأ تغيير في النطاق، فينبغي لمقاييس التأثير أن تعكس التأثير على سرية وحصانة وتيسر المكون الضعيف أو المكون المتأثر، أيهما يكون قد تعرض لأسوأ نتيجة.

#### 1.3.2.6 التأثير على السرية (C)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن ضعف على سرية موارد المعلومات التي يديرها مكون برمجية. وتشير السرية إلى تقييد النفاذ إلى المعلومات وعدم الكشف عنها إلا للمستخدمين المخولين، فضلاً عن منع المستخدمين غير المخولين من النفاذ إليها ومنع الإفصاح بها لهم. وترد قائمة بالقيم الممكنة في الجدول 6. وترتفع قيمة هذا المقياس كلما ازداد حجم فقدان سرية المكون المتأثر.

**الجدول 6 – التأثير على السرية**

| قيمة المقياس | الشرح |
|---|---|
| مرتفعة (H) | هناك فقدان تام للسرية بما يؤدي إلى حصول المهاجم على جميع الموارد الموجودة في المكون المتأثر. وإلا فيمكن النفاذ إلى بعض المعلومات السرية فقط إلا أن المعلومات المفشى عنها قد تعرضت لتأثير مباشر وخطير. وعلى سبيل المثال، يسرق مهاجم كلمة سر المسؤول أو مفتاح التشفير الخاص الذي يسمح بالدخول إلى مخدم الويب. |
| منخفضة (L) | تفقَّد السرية إلى حدّ ما. ويمكن النفاذ إلى بعض المعلومات السرية، إلا أن المهاجم لا يتحكم في ما يحصل عليه من معلومات أو أن حجم أو نوع الخسارة مقيد. ولا يتعرض المكون المتأثر لخسارة مباشرة وخطيرة بفعل إفشاء المعلومات. |
| معدومة (N) | ليس هناك فقدان للسرية ضمن المكون المتأثر. |

#### 2.3.2.6 التأثير على الحصانة (I)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن الضعف على الحصانة. وتشير الحصانة إلى جدارة المعلومات بالثقة وصدقها. وترد قائمة بالقيم الممكنة في الجدول 7. وتزداد قيمة هذا المقياس بازدياد التبعات على المكون المتأثر.

**الجدول 7 – التأثير على الحصانة**

| قيمة المقياس | الشرح |
|---|---|
| عالية (H) | هناك فقدان تام للحصانة أو فقدام كامل للحماية. فمثلاً، يستطيع المهاجم أن يعدّل أيًّا من/كل الملفات التي يحميها المكون المتأثر. وإلا فيمكن تعديل بعض الملفات فحسب، ولكن التعديلات الضارة سيكون لها تبعات مباشرة وفادحة على المكون المتأثر. |
| منخفضة (L) | إن تعديل البيانات ممكن ولكن المهاجم لا يتحكم بتبعات التعديل، أو إن حجم التعديل مقيّد. ولا يؤثر تعديل البيانات تأثيراً مباشراً وفادحاً على المكون المتأثر. |
| معدومة (N) | ليس هناك فقدان للحصانة ضمن المكون المتأثر. |

### 3.3.2.6 التأثير على التيسُّر (A)

يقيس هذا المقياس تأثير الاستغلال الناجح لموطن الضعف على تيسر المكون المتأثر. وفي حين ينطبق مقياسا التأثير على السرية والحصانة على فقدان سرية أو حصانة البيانات (كالمعلومات والملفات) التي يستخدمها المكون المتأثر، يرتبط هذا المقياس بفقدان تيسر المكون المتأثر عينه على غرار خدمة شبكية (مثل الويب وقاعدة البيانات والبريد الإلكتروني). وبما أن التيسر يشير إلى إمكانية النفاذ إلى موارد المعلومات، تؤثر كل الهجمات التي تستهلك عرض نطاق الشبكة أو دورات المعالج أو مساحة القرص على تيسر المكون المتأثر. وترد قائمة بالقيم الممكنة في الجدول 8. وتزداد قيمة هذا المقياس بازدياد التبعات على المكون المتأثر.

**الجدول 8 – التأثير على التيسر**

| قيمة المقياس | الشرح |
|---|---|
| مرتفعة (H) | هناك فقدان تام للتيسر بما يمكّن المهاجم من منع النفاذ إلى موارد المكون المتأثر منعاً تاماً؛ ويكون الفقدان إما متواصلاً (طالما يواصل المهاجم شن هجومه) أو دائماً (يدوم الوضع حتى بعد انتهاء الهجوم). وإلا فيستطيع المهاجم منع بعض التيسر غير أن فقدان التيسر له تبعات مباشرة وفادحة على المكون المتأثر (فمثلاً، لا يستطيع المهاجم قطع التوصيلات القائمة، ولكن يمكنه منع التوصيلات الجديدة؛ ويستطيع المهاجم أن يستغل مراراً وتكراراً موطن الضعف الذي يسرّب عند كل هجوم ناجح قدراً يسيراً من الذاكرة فقط، إلا أن الاستغلال المكرر يجعل الخدمة غير متيسرة البتة). |
| منخفضة (L) | هناك انخفاض في الأداء أو انقطاعات في تيسر الموارد. وحتى إن كان الاستغلال المكرر لموطن الضعف ممكناً، لا يتمتع المهاجم بالقدرة على حرمان المستخدمين المشروعين كلياً من الخدمة. وتكون موارد المكون المتأثر إما متيسرة جزئياً طوال الوقت، أو متيسرة كاملاً في بعض الأوقات فقط، ولكن على العموم لا توجد تبعات مباشرة وفادحة على المكون المتأثر. |
| معدومة (N) | لا تأثير على التيسر ضمن المكون المتأثر. |

## 3.6 المقاييس الزمنية

تقيس المقاييس الزمنية الحالة الحالية لتيسر تقنيات أو شفرة الاستغلال، أو وجود برمجيات تصحيحية أو حلول ترقيعية، أو الثقة بوصف موطن الضعف.

### 1.3.6 نضج شفرة الاستغلال (E)

يقيس هذا المقياس مدى احتمال مهاجمة موطن الضعف، ويستند عادةً إلى الحالة الحالية لتقنيات الاستغلال أو تيسر شفرة الاستغلال، أو الاستغلال الشائع النشط. ويزيد توافر شفرة سهلة الاستخدام للعموم لاستغلال مواطن الضعف عددَ المهاجمين المحتملين بتضمين أولئك غير المهرة منهم، مما يزيد من حدة موطن الضعف. وفي البداية، قد يكون استغلال مواطن الضعف أمراً نظرياً ليس إلا في العالم الحقيقي. ويمكن أن يلي ذلك نشر شفرة التنفيذ الأولي لمفهوم استغلال موطن الضعف أو الشفرة الوظيفية أو ما يكفي من التفاصيل التقنية اللازمة لاستغلال موطن الضعف. وعلاوةً على ذلك، يمكن أن تتطور شفرة الاستغلال المتاحة من بيان التنفيذ الأولي للمفهوم إلى شفرة استغلال تنجح في استغلال موطن الضعف باستمرار أو أدوات هجوم مؤتمتة أخرى. وفي الحالات الشديدة، يمكن تسليم هذه الشفرة كحمولة دودة أو فيروسة برمجية قائمة على الشبكة.

وترد قائمة بالقيم الممكنة في الجدول 9. وكلما سهل استغلال موطن الضعف، ارتفعت علامته.

**الجدول 9 – نضج شفرة الاستغلال**

| قيمة المقياس | الشرح |
|---|---|
| غير محددة (X) | إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى معادلة لحساب العلامة لتجاوز هذا المقياس. |
| مرتفعة (H) | توجد شفرة وظيفية مستقلة ذاتياً، أو لا لزوم للاستغلال (لتوفر مشغل يدوي) والتفاصيل متاحة على نطاق واسع. وتعمل شفرة الاستغلال في كل حالة، أو يجري إيصالها بنشاط عبر وكيل مستقل ذاتياً (مثل دودة أو فيروس). ويُرجح أن تكون الأنظمة الموصولة بالشبكات عرضة لمحاولات مسح أو استغلال. وأصبح تطوّر الاستغلال بمستوى الأدوات المؤتمتة الموثوق بها والمتوافرة على نطاق واسع والسهلة الاستخدام. |
| قابلة للتشغيل (F) | توفر شفرة استغلال قابلة للتشغيل. وتعمل الشفرة في معظم الحالات التي يوجد فيها موطن ضعف. |
| التنفيذ الأولي للمفهوم (P) | توفر شفرة التنفيذ الأولي للمفهوم أو لا يتمتع بيان للهجوم بقيمة عملية لمعظم الأنظمة. ويتعذر تشغيل الشفرة أو التقنية في معظم الحالات، وقد تتطلبان تعديلاً كبيراً من جانب مهاجم ماهر. |
| غير مثبتة (U) | لا تتوفر شفرة استغلال، أو أن الاستغلال نظري. |

### 2.3.6 مستوى التدارك (RL)

يُعدّ مستوى تدارك موطن الضعف عاملاً هاماً في تحديد الأولويات. ولا تكون الثغرة الأمنية مرقعةً عادةً عند نشرها في البداية. ويمكن للحلول الترقيعية السريعة أن تتدارك الثغرة مؤقتاً ريثما تصدر رقعة أو ترقية رسمية. وفي كل مرحلة من هذه المراحل المعنية، تعدَّل العلامة الزمنية تخفيضاً على نحو يعكس تناقص درجة التحسّب حتى يتم الاستدراك كلياً. وترد قائمة بالقيم الممكنة في الجدول 10. وكلما قل الطابع الرسمي والدائم للإصلاح، ارتفعت علامة موطن الضعف.

**الجدول 10 – مستوى التدارك**

| قيمة المقياس | الشرح |
|---|---|
| غير محددة (X) | إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى معادلة لحساب العلامة لتجاوز هذا المقياس. |
| غير متوفرة (U) | لا يتوفر حل أو يستحيل تطبيقه. |
| ترقيع سريع (W) | هناك حل غير رسمي صادر عن جهة غير الجهة البائعة. وفي بعض الحالات، سيبتكر مستخدمو التكنولوجيا المتضررة رقعتهم الخاصة أو سيقدمون سبلاً للالتفاف على موطن الضعف أو التخفيف من ضرره. |
| إصلاح مؤقت (T) | يتوفر إصلاح رسمي ولكنه مؤقت. ويشمل ذلك الحالات التي تُصدر فيها الجهة البائعة إصلاحاً مؤقتاً أو أداة أو ترقيعاً سريعاً. |
| إصلاح رسمي (O) | يتوفر حل كامل من الجهة البائعة. فإما أن تكون الجهة البائعة أصدرت رقعة رسمية، أو أن هناك ترقية متوفرة. |

### 3.3.6 الثقة في التقرير (RC)

يقيس هذا المقياس درجة الثقة في وجود موطن ضعف ومصداقية التفاصيل التقنية المعروفة. وفي بعض الأحيان، لا يُعلن على الملأ إلا عن وجود مواطن الضعف دون تفاصيل محددة. فمثلاً، قد يُعتبر التأثير تأثيراً غير مرغوب فيه مع جهل الأسباب الجذرية. ويمكن أن تدلّ البحوث لاحقاً على موطن الضعف بالإشارة إلى موضعه، مع أن البحوث قد لا تكون أكيدة. وأخيراً قد يتأكد وجود موطن الضعف بإقرار من الجهة المصدرة أو البائعة للتكنولوجيا المتأثرة. ويصبح موطن الضعف أكثر إلحاحاً عندما يُعرف وجوده على وجه اليقين. ويبيّن هذا المقياس أيضاً مستوى المعرفة التقنية المتاحة لمن يفكرون في الهجوم. وترد في الجدول 11 قائمة بالقيم الممكنة. وكلما تأكد وجود موطن الضعف من جانب الجهة البائعة أو مصادر موثوقة أخرى، ارتفعت العلامة.

**الجدول 11 – الثقة في التقرير**

| قيمة المقياس | الشرح |
|---|---|
| غير محددة (X) | إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى معادلة لحساب العلامة لتجاوز هذا المقياس. |
| مؤكدة (C) | هناك تقارير مفصلة أو يمكن إجراء نسخة وظيفية (يمكن للاستغلال الوظيفي أن يوفر ذلك). وتتوافر شفرة للمصدر للتحقق بصورة مستقلة من تأكيدات البحوث، أو أكدت الجهة المصدرة أو البائعة للشفرة المتضررة وجود موطن الضعف. |
| معقولة (R) | تُنشر تفاصيل عديدة ولكن الباحثين لا يثقون تمام الثقة بالسبب الجذري، أو لا يمكنهم النفاذ إلى شفرة المصدر للتأكد تماماً من جميع التفاعلات التي قد تفضي إلى هذه النتيجة. ولكن هناك ثقة معقولة في أن الثغرة يمكن أن تتكرر وأنه يمكن التحقق من أثر واحد على الأقل (يمكن أن يوفر استغلال التنفيذ الأولي للمفهوم ذلك). ومن الأمثلة على ذلك، دراسة مفصلة تبحث في موطن الضعف مع شرح (ربما مموه أو "متروك كتمرين للقارئ") يضمن تكرار النتائج. |
| مجهولة (U) | هناك تقارير عن آثار تدل على وجود موطن ضعف. وتُظهر التقارير أن سبب الضعف مجهول، أو قد لا تتفق التقارير على أسباب الضعف أو آثاره. ومحررو التقارير غير متأكدين من الطبيعة الحقيقية لموطن الضعف، وتقلّ الثقة في صحة التقارير أو فيما إذا أمكن تطبيق علامة قاعدية جامدة نظراً إلى الاختلافات المذكورة. ومن الأمثلة على ذلك، تقرير عن الثغرات يلاحظ حدوث عطل متقطع ولكن لا يمكن تكراره، مع وجود أدلة على وقوع تلف في الذاكرة يشير إلى أن الأمر قد يؤدي إلى الحرمان من الخدمة أو إلى آثار أخطر ممكنة. |

### 4.6 المقاييس البيئية

تمكّن هذه المقاييس المحلل من أن يكيّف علامة نظام تحديد درجات لمواطن الضعف الشائعة تبعاً لأهمية مقتنيات تكنولوجيا المعلومات والاتصالات المتضررة في منظمة المستخدم، من حيث الضوابط الأمنية المكملة/البديلة الموجودة والسرية والحصانة والتيسر. وتمثل هذه المقاييس المقابل المعدَّل للمقاييس القاعدية وتُسند إليها قيم بناء على موقع المكون في البنية التحتية للمنظمة.

#### 1.4.6 متطلبات الأمن (CR، IR، AR)

تمكّن هذه المقاييس المحلل من أن يكيّف علامة نظام تحديد درجات لمواطن الضعف الشائعة تبعاً لأهمية مقتنيات تكنولوجيا المعلومات والاتصالات المتضررة في منظمة المستخدم من حيث السرية والحصانة والتيسر. فإذا كان أحد مقتنيات تكنولوجيا المعلومات والاتصالات داعماً لوظيفة تجارية تولي أهمية قصوى للتيسر، يستطيع المحلل أن يسند قيمة أكبر للتيسر نسبة إلى السرية والحصانة. ولكل من متطلبات الأمن ثلاث قيم محتملة: منخفضة أو متوسطة أو مرتفعة.

ويُحدَّد التأثير الكامل على العلامة البيئية بما يقابل من مقاييس التأثير القاعدية المعدَّلة. وهذا يعني أن هذه المقاييس تعدل العلامة البيئية من خلال إعادة ترجيح مقاييس التأثير المعدَّل على السرية والحصانة والتيسر. فعلى سبيل المثال، يزداد رجحان مقياس التأثير على السرية المعدَّل (MC) إذا كان متطلب السرية (CR) مرتفعاً. وبالمثل، ينخفض رجحان مقياس التأثير على السرية المعدَّل إذا كان متطلب السرية منخفضاً. ويكون رجحان مقياس التأثير على السرية المعدَّل حيادياً إذا كان متطلب السرية متوسطاً. ويسري هذا المنطق نفسه على متطلبات الحصانة والتيسر.

وجدير بالذكر أن متطلب السرية لن يؤثر على العلامة البيئية إذا ما انعدم التأثير على السرية (القاعدي المعدَّل). كما أن زيادة متطلب السرية، من متوسط إلى مرتفع، لن تغير العلامة البيئية عندما تُسند قيمة عالية لمقاييس التأثير (القاعدي المعدل). وذلك لأن العلامة الفرعية للتأثير المعدلة (جزء من العلامة القاعدية المعدلة التي تحسب التأثير) بلغت فعلاً قيمة 10 القصوى.

وترد في الجدول 12 قائمة بالقيم الممكنة. وللإيجاز، يستخدم الجدول نفسه لجميع المقاييس الثلاثة. وكلما ارتفع متطلب الأمن، ارتفعت العلامة (علماً بأن القيمة المتوسطة هي القيمة الغيابية).

**الجدول 12 – متطلبات الأمن**

| قيمة المقياس | الشرح |
|---|---|
| غير محددة (X) | إسناد هذه القيمة إلى المقياس لن يؤثر على العلامة. بل هو إشارة إلى المعادلة لتجاوز هذا المقياس. |
| مرتفعة (H) | يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً كارثياً على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء). |
| متوسطة (M) | يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً جداً على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء). |
| منخفضة (L) | يرجح أن يؤثر فقدان [السرية/الحصانة/التيسر] تأثيراً سلبياً محدوداً فقط على المنظمة أو الأفراد المرتبطين بها (مثل الموظفين والعملاء). |

### 2.4.6 المقاييس القاعدية المعدَّلة

تمكّن هذه المقاييس المحلل من أن يكيّف المقاييس القاعدية تبعاً للتعديلات التي تطرأ على بيئة المحلل. وعليه، فإذا أحدثت بيئة ما تغيرات عامة على البرمجية المتضررة التي ستتبدّل بما يؤثر على إمكانية استغلالها أو نطاقها أو تأثيرها، يمكن أن تُظهر البيئة ذلك بتعديل العلامة البيئية تعديلاً ملائماً.

ويُحدَّد التأثير الكامل على العلامة البيئية بما يقابلها من مقاييس قاعدية. وهذا يعني أن هذه المقاييس تعدل العلامة البيئية من خلال إعادة إسناد قيم المقاييس (القاعدية)، قبل تطبيق متطلبات الأمن (البيئة). فعلى سبيل المثال، قد تكون التشكيلة العادية لمكون ضعيف هي تشغيل خدمة سمعية مع التمتع بامتيازات المسؤول وقد يفضي الحل الوسط في هذا الشأن إلى منح المهاجم القدرة على التأثير على كل من السرية والحصانة والتيسر تأثيراً عالياً. ولكن قد تكون خدمة الإنترنت نفسها المستخدمة في بيئة المحلل مشغَّلة بامتيازات مخفضة؛ وفي هذه الحالة، يمكن أن يخفض مستوى كل من السرية المعدلة والحصانة المعدلة والتيسر المعدل.

وباختصار، لا يُذكر سوى أسماء المقاييس القاعدية المعدلة. وتبلغ قيمة كل مقياس بيئي معدل القيمة نفسها بما يقابله من مقياس قاعدي زائد قيمة غير محددة.

والغرض من هذا المقياس هو تحديد مظاهر التخفيف القائمة في بيئة معينة. واستخدام المقاييس المعدلة لوصف الحالات التي ترفع العلامة القاعدية أمر مقبول. فعلى سبيل المثال، قد تكون التشكيلة العادية لمكون ما هي اقتضاء امتيازات عالية (الامتيازات المطلوبة: عالية) بغية النفاذ إلى وظيفة معينة، ولكن قد لا تكون هناك امتيازات مطلوبة في بيئة المحلل (الامتيازات المطلوبة: معدومة). ويمكن أن يحدّد المحلل أن "الامتيازات المعدَّلة المطلوبة: معدومة" لبيان هذا الوضع الأخطر لبيئتها.

وترد في الجدول 13 قائمة بالقيم الممكنة.

**الجدول 13 – المقاييس القاعدية المعدلة**

| المقياس القاعدي المعدل | القيم المقابلة |
|---|---|
| متجه الهجوم المعدّل (MAV) | القيم ذاتها لما يقابلها من مقاييس قاعدية (انظر المقاييس القاعدية أعلاه) وغير محددة (عادية). |
| تعقيد الهجوم المعدَّل (MAC) | |
| الامتيازات المطلوبة المعدَّلة (MPR) | |
| تفاعل المستخدم المعدّل (MUI) | |
| النطاق المعدّل (MS) | |
| السرية المعدَّلة (MC) | |
| الحصانة المعدَّلة (MI) | |
| التيسّر المعدَّل (MA) | |

### 5.6 سلّم التصنيف النوعي للحدة

من المفيد لبعض الأغراض وضع تمثيل نصي للعلامات الرقمية القاعدية والزمنية والبيئية. ويمكن إدراج جميع العلامات في إطار التصنيف النوعي المحدد في الجدول 14.[3]

**الجدول 14 – سلّم التصنيف النوعي للحدة**

| التصنيف | علامة CVSS |
|---|---|
| معدومة | 0,0 |
| منخفضة | 3,9-0,1 |
| متوسطة | 6,9-4,0 |
| مرتفعة | 8,9-7,0 |
| حرجة | 10,0-9,0 |

وعلى سبيل المثال، إذا كانت العلامة القاعدية لنظام تحديد درجات لمواطن الضعف الشائعة تبلغ 4,0، يكون تصنيف الحدة المرتبط بها "متوسطاً". واستخدام هذا التصنيف النوعي للحدة أمر اختياري، كما أن ذكره عند نشر علامات نظام تحديد درجات لمواطن الضعف الشائعة ليس إلزامياً. والغرض من هذا التصنيف هو مساعدة المنظمات على القيام بشكل مناسب بتقييم العمليات التي تتبعها لإدارة مواطن الضعف وترتيبها من حيث الأولوية.

### 6.6 سلسلة المتجهات

إن سلسلة متجهات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة هو تمثيل نصي لمجموعة من مقاييس هذا النظام. وتُستخدم عادةً لتسجيل أو نقل معلومات عن مقاييس نظام تحديد درجات لمواطن الضعف الشائعة بشكل موجز.

وتبدأ سلسلة متجهات الإصدار 3.0 بالمختصر "CVSS:" وبتمثيل رقمي عن الإصدار الحالي "3.0"، وتتبع ذلك معلومات عن المقاييس في شكل مجموعة مقاييس يُوضع قبل كل مقياس الخط المائل "/" لفصل المقاييس. ويتألف كل مقياس في المتجه من الاسم المختصر للمقياس متبوعاً بنقطتين ":" ثم بقيمة المقياس المختصرة المرتبطة به. وتحدَّد الأشكال المختصرة مسبقاً على هذا النحو (بين هلالين وبعد اسم المقياس وقيمته) وهي موجزة في الجدول أدناه.

ويمكن أن تُحدد المقاييس بأي ترتيب كان في سلسلة المتجهات، إلا أن الجدول 15 يُظهر الترتيب المحبذ. ويجب إدراج جميع المقاييس القاعدية في سلسلة متجهات. والمقاييس الزمنية والبيئية هي مقاييس اختيارية، وتُسند إلى المقاييس المحذوفة قيمة "غير محددة (X)". ويمكن إدراج المقاييس ذات القيمة غير المحددة صراحة في سلسلة متجهات حسب الاقتضاء. ويجب أن تقبل البرامج التي تقرأ سلاسل متجهات الإصدار 3.0 المقاييس أياً كان ترتيبها وأن تعالج المقاييس الزمنية والبيئية غير المحددة باعتبارها ذات قيمة "غير محددة". ولا يجوز لسلسلة متجهات واحدة أن تتضمن المقياس ذاته أكثر من مرة واحدة.

[3] يرجى ملاحظ أنه من الممكن تقسيم العلامات إلى علامات كمية ونوعية سواء كان يتم تقييم المقياس القاعدي فقط أو كامل مجموعة المقاييس القاعدية والزمنية والبيئية.

**الجدول 15 – المتجهات القاعدية والزمنية والبيئية**

| فئة المقياس | اسم المقياس ومختصره باللغة الإنكليزية | القيم الممكنة | هل هو إلزامي؟ |
|---|---|---|---|
| قاعدي | متجه الهجوم، AV | [N,A,L,P] | نعم |
| | تعقيد الهجوم، AC | [L,H] | نعم |
| | الامتيازات المطلوبة، PR | [N,L,H] | نعم |
| | تفاعل المستخدم، UI | [N,R] | نعم |
| | النطاق، S | [U,C] | نعم |
| | السرية، C | [H,L,N] | نعم |
| | الحصانة، I | [H,L,N] | نعم |
| | التيسر، A | [H,L,N] | نعم |
| زمني | نضج شفرة الاستغلال، E | [X,H,F,P,U] | لا |
| | مستوى التدارك، RL | [X,U,W,T,O] | لا |
| | الثقة في التقرير، RC | [X,C,R,U] | لا |
| بيئي | متطلب السرية، CR | [X,H,M,L] | لا |
| | متطلب الحصانة، IR | [X,H,M,L] | لا |
| | متطلب التيسر، AR | [X,H,M,L] | لا |
| | متجه الهجوم المعدّل، MAV | [X,N,A,L,P] | لا |
| | تعقيد الهجوم المعدَّل، MAC | [X,L,H] | لا |
| | الامتيازات المطلوبة المعدَّلة، MPR | [X,N,L,H] | لا |
| | تفاعل المستخدم المعدّل، MUI | [X,N,R] | لا |
| | النطاق المعدل، MS | [X,U,C] | لا |
| | السرية المعدلة، MC | [X,N,L,H] | لا |
| | الحصانة المعدلة، MI | [X,N,L,H] | لا |
| | التيسر المعدل، MA | [X,N,L,H] | لا |

ومثلاً، موطن الضعف ذو قيم المقاييس القاعدية التالية: "متجه الهجوم: شبكة، تعقيد الهجوم: منخفضة، الامتيازات المطلوبة: مرتفعة، تفاعل المستخدم: معدومة، النطاق: ثابتة، السرية: منخفضة، الحصانة: منخفضة، التيسر: معدومة" ودون مقاييس زمنية أو بيئية محددة، سيكون له المتجه التالي:

– CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

وإذا أخذنا المثال ذاته وأضفنا إليه "إمكانية الاستغلال: قابلة للتشغيل، مستوى التدارك: غير محدد" وعرضنا المقياس بترتيب غير محبذ، سيكون المتجه على الشكل التالي:

CVSS:3.0/S:U/AV:N/AC:L/PR:H/UI:N/C:L/I:L/A:N/E:F/RL:X

### 7.6 تعريف مخطط لغة الوسم القابلة للتوسيع XML (XSD) المتعلق بالإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة

يحدِّد تعريف مخطط لغة الوسم القابلة للتوسيع XML (XSD) المتعلق بنظام تحديد درجات لمواطن الضعف الشائعة بنيةَ ملف لغة الوسم القابلة للتوسيع الذي يتضمن قيم مقاييس نظام تحديد درجات لمواطن الضعف الشائعة، وهو مفيد للراغبين في تخزين أو نقل هذه البيانات بلغة الوسم القابلة للتوسيع. وهذا التعريف متاح في العنوان التالي: https://www.first.org/cvss/cvss-v3.0.xsd

### 8.6 معادلات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة

تحدّد أدناه معادلات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

#### 1.8.6 المعادلة القاعدية

العلامة القاعدية هي وظيفة من معادلات العلامتين الفرعيتين للتأثير وإمكانية الاستغلال. فتحدد العلامة القاعدية على النحو التالي:

| | |
|---|---|
| *If (Impact sub score <= 0)* | *0 else,* |
| *Scope Unchanged* [4] | $Roundup(Minimum[(Impact + Exploitability), 10])$ |
| *Scope Changed* | $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$ |

وتحدد العلامة الفرعية للتأثير (ISC) على النحو التالي:

*Scope Unchanged* $6.42 \times ISC_{Base}$

*Scope Changed* $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

حيث،

$$ISC_{Base} = 1 - \left[\left(1 - Impact_{Conf}\right) \times \left(1 - Impact_{Integ}\right) \times \left(1 - Impact_{Avail}\right)\right]$$

وتحدد العلامة الفرعية لإمكانية الاستغلال على النحو التالي:

$$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$$

#### 2.8.6 المعادلة الزمنية

تحدَّد العلامة الزمنية على النحو التالي:

$$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$$

[4] حيث يُعتبر "Round up" الرقم الأصغر المحدد بعلامة عشرية واحدة وهو يساوي مدخلاته أو يزيد عنها. فمثلاً، Round up (4.02) يساوي 4.1؛ وRound up (4.00) يساوي 4.0.

### 3.8.6 المعادلة البيئية

تحدَّد العلامة البيئية على النحو التالي:

| | |
|---|---|
| *If (Modified Impact Sub score <= 0)* | 0 else, |
| *If Modified Scope is Unchanged* | *Round up(Round up (Minimum [ × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)* |
| *If Modified Scope is Changed* | *Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)* |

وتُحدّد العلامة الفرعية للتأثير على النحو التالي:

| | |
|---|---|
| *If Modified Scope is Unchanged* | $6.42 \times \left[ISC_{Modified}\right]$ |
| *If Modified Scope is Changed* | $7.52 \times \left[ISC_{Modified} - 0.029\right]$ -3.25 $\times \left[ISC_{Modified} - 0.02\right]^{15}$ |

حيث،

$$ISC_{Modified} = Minimum\left[\left[1 - \left(1 - M.I_{Conf} \times CR\right) \times \left(1 - M.I_{Integ} \times IR\right) \times \left(1 - M.I_{Avail} \times AR\right)\right], 0.915\right]$$

وتُحدَّد العلامة الفرعية لإمكانية الاستغلال المعدلة على النحو التالي:

$$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$$

### 4.8.6 مستويات المقاييس

تحدد قيم المقاييس في الجدول 16.

**الجدول 16 – قيم المقاييس**

| المقياس | قيمة المقياس | القيمة الرقمية |
|---|---|---|
| متجه الهجوم/متجه الهجوم المعدَّل | شبكة | 0,85 |
| | شبكة مجاورة | 0,62 |
| | محلية | 0,55 |
| | مادية | 0,2 |
| تعقيد الهجوم/تعقيد الهجوم المعدَّل | منخفضة | 0,77 |
| | عالية | 0,44 |
| الامتيازات المطلوبة/الامتيازات المطلوبة المعدَّلة | معدومة | 0,85 |
| | منخفضة | 0,62 (0,68 إذا تغيّر النطاق/النطاق المعدَّل) |
| | مرتفعة | 0,27 (0,50 إذا تغيّر النطاق/النطاق المعدَّل) |
| تفاعل المستخدم/تفاعل المستخدم المعدَّل | معدومة | 0,85 |
| | ضرورية | 0,62 |
| تأثير C,I,A/تأثير C,I,A المعدَّل | مرتفعة | 0,56 |
| | منخفضة | 0,22 |
| | معدومة | 0 |
| نضج شفرة الاستغلال | غير محددة | 1 |
| | مرتفعة | 1 |
| | قابلة للتشغيل | 0,97 |
| | التنفيذ الأولي للمفهوم | 0,94 |
| | غير مثبتة | 0,91 |
| مستوى التدارك | غير محددة | 1 |
| | غير متوفرة | 1 |
| | ترقيع سريع | 0,97 |
| | إصلاح مؤقت | 0,96 |
| | إصلاح رسمي | 0,95 |
| الثقة في التقرير | غير محددة | 1 |
| | مؤكدة | 1 |
| | معقولة | 0,96 |
| | مجهولة | 0,92 |
| متطلبات الأمن – متطلبات C,I,A (CR) | غير محددة | 1 |
| | مرتفعة | 1,5 |
| | متوسطة | 1 |
| | منخفضة | 0,5 |

### 5.8.6 لمحة عن معادلات وعلامات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة

توفّر صيغة الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة تقديراً حسابياً تقريبياً لجميع التركيبات المحتملة بين المقاييس والمرتبة بحسب حدتها (جدول بحث عن موطن الضعف). ومن أجل إنتاج صيغة الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، أعدت مجموعة المصالح الخاصة (SIG) جدول البحث بإسناد قيم مقاييس الإصدار 3.0 إلى مواطن ضعف حقيقية وفئة من فئات الحدة (منخفضة أو متوسطة أو مرتفعة أو حرجة). وإذ حَددت المجموعة النطاقات الرقمية المقبولة لكل مستوى من مستويات الحدة، تعاونت بعد ذلك مع شركة "Deloitte & Touche LLP" لتكييف معلمات الصيغة من أجل مواءمة تركيبات مقاييس الإصدار 3.0 مع التصنيف الذي اقترحته المجموعة لمستويات الحدة.

ونظراً إلى العدد المحدود للنواتج الرقمية (101 ناتج تتراوح بين 0,0 و10,0)، يمكن أن تنتج التركيبات المتعددة لحساب العلامات العلامة الرقمية ذاتها. وفضلاً عن ذلك، يمكن حذف بعض العلامات الرقمية لأن الترجيحات والحسابات مستخلصة من تصنيف تركيبات المقاييس بحسب الحدة. وعلاوة على ذلك، قد تحيد تركيبات المقاييس في بعض الحالات عن الحد الأدنى المرجو للحدة. ولا يمكن تفادي هذا الأمر كما لا يسهل إجراء تصحيح بسيط لأن التعديلات المدخلة على إحدى قيم المقاييس أو معلمة معادلة لتصحيح الانحراف ستتسبب بانحرافات أخرى قد تكون أكثر حدة.

وعلى غرار الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة، اصطُلح على أن يكون الانحراف المقبول بقيمة 0,5. ومن هنا، ستنتج جميع تركيبات قيم المقاييس المستخدمة لاستخلاص الترجيحات والحسابات علامة رقمية ضمن مستوى الحدة المسند إليها أو ضمن 0,5 من هذا المستوى المسند. فمثلاً، قد تتراوح العلامة الرقمية للتركيبة التي يُتوقع تصنيفها على أنها "عالية" بين 6,6 و9,3. وختاماً، يحتفظ الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة بالنطاق المتراوح بين 0,0 و10,0 للتوافق الرجعي.

# التذييل I

## دليل مستخدمي الإصدار 3.0 لنظام تحديد درجات لمواطن الضعف الشائعة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

### 1.I مقدمة

يكمّل هذا الدليل الوثيقة الرسمية المتعلقة بمواصفات الإصدار 3.0 لنظام تحديد درجات لمواطن الضعف الشائعة فيوفّر المزيد من المعلومات ويُلقي الضوء على التغيرات الهامة مقارنة بالإصدار 2.0 ويوفّر الإرشاد لوضع العلامات ويتضمن جزءاً عن وضع العلامات.

ويحدّد نظام تحديد درجات لمواطن الضعف الشائعة طريقة استخلاص الخصائص الرئيسية لمواطن الضعف وإنتاج علامة رقمية تبيّن حدة موطن الضعف وتمثيل نصي لهذه العلامة. ويصبح عندئذ من الممكن ترجمة العلامة الرقمية إلى تمثيل نوعي (مثلاً قيمة منخفضة أو متوسطة أو مرتفعة أو حرجة) لمساعدة المنظمات على القيام بشكل مناسب بتقييم العمليات التي تتبعها لإدارة مواطن الضعف وترتيبها من حيث الأولوية.

ولنظام تحديد درجات لمواطن الضعف الشائعة ثلاث منافع هامة هي:

- يتيح تحديد علامات موحدة لمواطن الضعف. فعندما تستخدم منظمة خوارزمية واحدة لحساب علامات مواطن الضعف لجميع منصات تكنولوجيا المعلومات والاتصالات، يمكنها الاستفادة من سياسة موحدة لإدارة مواطن الضعف تنص على المدة القصوى المسموح بها للتحقق من مواطن ضعف معينة وتداركها.
- يوفّر إطاراً مفتوحاً. فقد يختلط الأمر على المستخدم عندما يُسند طرف ثالث علامة اعتباطية لموطن الضعف. وباستخدام نظام تحديد درجات لمواطن الضعف الشائعة يمكن لأيّ كان الاطلاع على الخصائص الفردية المستخدمة لاستخلاص العلامة.
- يساعد على ترتيب المخاطر من حيث الأولوية. فعند حساب العلامة البيئية، يصبح موطن الضعف سياقياً لكل منظمة، ويساعد على تحسين فهم المخاطر التي تحدق بالمنظمة نتيجة موطن الضعف.

ويتم اعتماد نظام تحديد درجات لمواطن الضعف الشائعة على نطاق واسع منذ إطلاقه للمرة الأولى عام 2004. وفي سبتمبر 2007، اعتُمد الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة كجزء من معيار أمن بيانات قطاع بطاقات الدفع (PCI DSS). ومن أجل الوفاء بمعيار أمن بيانات قطاع بطاقات الدفع، على جميع التجار المتعاملين مع بطاقات ائتمان أن يثبتوا أن أنظمتهم الحاسوبية لا يشوبها أي موطن ضعف تساوي علامته في نظام تحديد درجات لمواطن الضعف الشائعة 4.0 أو أكثر. وأدرج المعهد الوطني للمعايير والتكنولوجيا (NIST) في عام 2007 الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة في بروتوكول أتمتة المحتوى الأمني (SCAP)[5]. وفي أبريل 2011، اعتُمد رسمياً الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة بوصفه معياراً دوليًا لحساب علامات مواطن الضعف (ITU-T X.1521)[6].

### 2.I التعديلات في الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة

نظراً إلى اعتماد الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة على نطاق واسع، حُدد عدد من الفرص لتحسين النظام مما حثّ على وضع الإصدار 3.0. ويرد وصفها بالتفصيل فيما يلي.

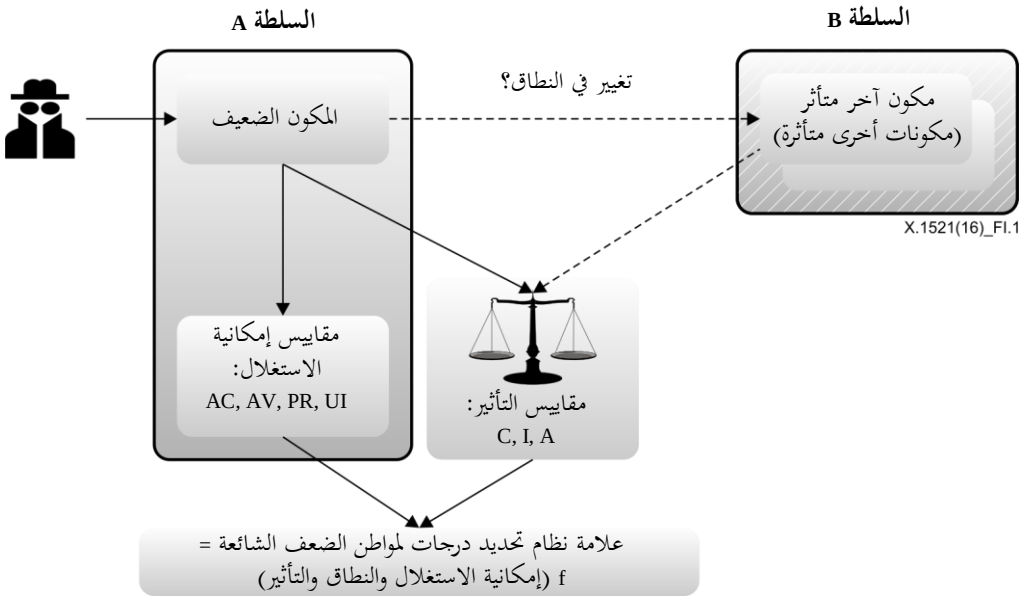
---

5 انظر http://scap.nist.gov/.

6 انظر https://www.itu.int/rec/T-REC-X.1521-201104-I/en.

### 1.2.I النطاق والمكون الضعيف والمكون المتأثر

كان البائعون يواجهون مشاكل مع الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة عند حساب علامات مواطن الضعف التي من شأنها أن تعطّل برمجيتهم بالكامل وألا تؤثر سوى جزئياً على نظام التشغيل المضيف. ففي الإصدار 2.0، توضع علامات مواطن الضعف بالاعتماد على نظام التشغيل المضيف، مما دفع أحد باعة التطبيقات إلى اعتماد اتفاقية مقياس التأثير.[7] "Partial+" ويعالج الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة هذه المشكلة بإدخال تحديثات تتعلق بالموقع الذي تُحسب فيه علامات مقاييس التأثير واستحداث مقياس جديد يسمى النطاق (جرى بحثه أدناه). ومن هنا، فإن أحد التغيرات النظرية الهامة في الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة هو إمكانية وضع علامات لمواطن الضعف التي تعتري أحد مكونات برمجية ما (والتسمية الرسمية التي تطلق عليه هي *المكون الضعيف*) والتي تؤثر مع ذلك على مكون برمجية أو معدة أو شبكة منفصلة (والتسمية الرسمية التي تطلق عليه هي *المكون المتأثر*)، على النحو الموضح في الرسم 1.I.[8]




**الشكل 1.I – تغير النطاق**

ولنأخذ مثال موطن ضعف في آلة افتراضية يعطّل نظام التشغيل المضيف. إن المكون الضعيف هو الآلة الافتراضية، في حين أن المكون المتأثر هو نظام التشغيل المضيف. ويدير هذان المكونان بصورة منفصلة امتيازات للموارد الحاسوبية، وبالتالي، يمثلان سلطتين مستقلتين (للتخويل). وفي الرسم 1.I، تدير "السلطة A" الآلة الافتراضية في حين تدير "السلطة B" نظام التشغيل المضيف. وعندما تشارك سلطتان في استغلال أحد مواطن الضعف، يعتبر نظام تحديد درجات لمواطن الضعف الشائعة أن هناك *تغيراً في النطاق*. ويستخلص مقياسُ "النطاق" الجديد هذا الوضع.

وعلى النحو المبيّن في الرسم 1.I، فعند وضع علامات لمواطن الضعف بواسطة الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، تحسب علامة مقاييس إمكانية الاستغلال نسبة إلى المكون الضعيف. أي إن العلامة توضع بالنظر إلى المكون الذي يشكو من عيب في التشفير. ومن جهة أخرى، تُحسب علامة مقاييس التأثير نسبة إلى المكون المتأثر. وفي بعض الأحيان، قد يكون المكون الضعيف هو المكون المتأثر أيضاً، وفي هذه الحالة لا يطرأ أي تغيير على النطاق. ولكن في أحيان أخرى، قد يتأثر المكون الضعيف إضافة إلى المكون المتأثر. وفي هذه الحالات، يطرأ تغيير على النطاق وينبغي لمقاييس التأثير على السرية والحصانة والتيسر أن تعكس التأثير على المكون الضعيف أو المكون المتأثر باختيار الذي تعرض للتأثير الأكبر.

---

7 انظر مثلاً http://www.oracle.com/technetwork/topics/security/cvssscoringsystem-091884.html.

8 يرجى ملاحظة أن المكون الضعيف هو برمجية (نظام تشغيل مضيف أو تطبيق للإنترنت أو محرك جهاز أو غير ذلك)، في حين أن المكون المتأثر هو إما برمجية أخرى أو معدة أخرى أو مورد شبكي آخر.

وفي حالة موطن ضعف يسمح بسرقة ملف لكلمات سر، وفي حين قد يتخذ المهاجم خطوات لاحقة للنفاذ غير المصرح به إلى الحسابات، فإن النتيجة المباشرة هي فقدان سرية ملف النظام المحلي. وفي هذه الحالة، لن يحدث تغير في النطاق. ولكن في حالة موطن ضعف يسمح للمهاجم باستبدال جدول بروتوكول استبانة العنوان في ميسر فإن للأمر تأثيرين، أولهما على ملف نظام الميسر (التأثير على حصانة المكون الضعيف) وثانيهما على خدمات الإنترنت التي يوفرها الميسر (التأثير على تيسر الأنظمة المتضررة). وينبغي للعلامة أن تعكس النتيجة الأسوأ ولذلك قد تعكس علامة مقاييس التأثير إما فقدان المكون الضعيف للحصانة أو فقدان تيسر خدمات الإنترنت، باختيار ما تعرض للتأثير الأكبر.[9]

### 2.2.I متجه النفاذ

أعيد تسمية متجه النفاذ (الموجود في الإصدار 2.0) ليصبح متجه الهجوم، إلا أنه ما زال يعكس بشكل عام "بُعد" المهاجم عن المكون الضعيف. وعليه، فكلما ابتعد المهاجم عن المكون الضعيف (من حيث المسافة الشبكية المنطقية والمادية)، ترتفع العلامة القاعدية. وبالإضافة إلى ذلك، يميّز هذا المقياس الآن بين الهجمات المحلية التي تستلزم النفاذ إلى النظام المحلي (مثل هجوم على تطبيق مكتبي) والهجمات المادية التي تستلزم النفاذ مادياً إلى المنصة من أجل استغلال موطن الضعف (مثل هجوم عبر Firewire أو الناقل التسلسلي الشامل (USB) أو هجوم بإزالة الحواجز في جهاز).

### 3.2.I تعقيد الهجوم

كان تعقيد النفاذ (الموجود في الإصدار 2.0) يجمع بين مسألتين هما: أي وضع في البرمجية أو المعدة أو الشبكة لا يتحكم به المهاجم وينبغي أن يكون موجوداً أو واقعاً للتمكن من استغلال موطن الضعف بنجاح (مثل وجود شرط تزامني في البرمجية أو تشكيلة تطبيق) وضرورة وجود تفاعل بشري (مثل ضرورة قيام مستخدم بتشغيل برنامج مضرّ قابل للتشغيل). وبالتالي، قُسم تعقيد النفاذ إلى مقياسين منفصلين هما تعقيد الهجوم (الذي يتناول الحالة الأولى) و**تفاعل المستخدم** (الذي يتناول الحالة الثانية).

### 4.2.I الامتيازات المطلوبة

يحل مقياس **الامتيازات المطلوبة** الجديد محل مقياس الاستيقان (الموجود في الإصدار 2.0). فعوضاً عن قياس *عدد المرات* التي يقوم فيها نظام باستيقان المهاجم على نحو منفصل، تستخلص الامتيازات المطلوبة *مستوى النفاذ* المطلوب لنجاح الهجوم. وبوجه خاص، تعكس قيم المقاييس المرتفعة والمنخفضة والمعدومة الامتيازات المطلوبة من مهاجم ليتمكن من استغلال موطن الضعف.

### 5.2.I مقاييس التأثير

إن قيم مقاييس التأثير على **السرية** و**الحصانة** و**التيسر**، الموجودة في الإصدار 2.0، والمتمثلة في "معدومة" و"جزئية" و"كاملة" استبدلت بالقيم "معدومة" و"منخفضة" و"مرتفعة". وعوضاً عن تمثيل *النسبة المئوية* (النسبة) الإجمالية للأنظمة المتضررة من جراء الهجوم، تعكس قيم المقاييس الجديدة *الدرجة* الإجمالية للتأثير الذي خلفه الهجوم. وعلى سبيل المثال، أدى موطن الضعف "Heartbleed"[10] إلى فقدان القليل من المعلومات فقط، إلا أن تأثيره كان شديداً. وفي الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة، لكان قد حظي بعلامة قيمتها "جزئية" في حين يمنحه الإصدار 3.0 علامة قيمتها "مرتفعة" وهي العلامة المناسبة.

وبالإضافة إلى ذلك، تعكس الآن مقاييس التأثير، في المثل أعلاه، التبعات على المكون المتأثر. وقد لا يكون المكون المتأثر هو ذاته المكون الذي يعالج موطن الضعف الذي يُستغل.

### 6.2.I المقاييس الزمنية

جرى التقليل من أثر المقاييس الزمنية في الإصدار 3.0 مقارنة بالإصدار 2.0. وأعيد تسمية "إمكانية الاستغلال" لتصبح "نضج شفرة الاستغلال" كي تمثل بشكل أفضل ما تقيسه المقاييس.

---

9 انظر وثيقة الأمثلة المرفقة بهذا الدليل للحصول على مزيد من المعلومات.

10 انظر http://heartbleed.com/.

### 7.2.I المقاييس البيئية

استعيض عن المقاييس البيئية لتوزع الأهداف والأضرار الجانبية المحتملة بالعوامل المعدَّلة التي تتضمن الضوابط المخففة للتأثير أو الثغرات في الضوابط مما قد يشوب بيئة المستخدم التي يمكن أن تخفف أو تزيد من تأثير مواطن الضعف المستغَلة بنجاح.

### 8.2.I سلّم التصنيف النوعي

أنشأت بعض المنظمات أنظمة لربط العلامات القاعدية في الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة بتصنيف نوعي. ويوفّر الإصدار 3.0 الآن مخططاً معيارياً لربط العلامات الرقمية بالصفات المستخدمة لتصنيف الحدة وهي "معدومة" و"منخفضة" و"متوسطة" و"مرتفعة" و"حرجة"، على النحو الموضح في وثيقة مواصفات الإصدار 3.0. واستخدام هذا التصنيف النوعي للحدة أمر اختياري، كما أن ذكره عند نشر علامات نظام تحديد درجات لمواطن الضعف الشائعة ليس إلزامياً.

أما المنظمات التي تستخدم علامات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة والتي ترغب في اعتماد نظام *بديل* لتصنيف الحدة، فيُطلب منها استخدام مفردات مختلفة للتصنيف أو الإشارة بوضوح إلى أن تصنيفها لا يتقيد بمواصفة الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، وذلك تفادياً لأي التباس.

### 9.2.I لمحة عن التغيرات

من أبرز نتائج هذه التغيرات أن علامات الإصدارين 2.0 و3.0 قد لا تكون دائماً قابلة للمقارنة. فمثلاً لكان قد حظي تطبيق ضعيف يمكن أن يؤدي إلى تعطيله كلياً بعلامة قيمتها "جزئية" في إطار قيم مقاييس التأثير على السرية والحصانة والتيسر في الإصدار 2.0. في حين سيحظى موطن الضعف ذاته الآن بعلامة قيمتها "عالية" في إطار القيم المماثلة لمقاييس التأثير على السرية والحصانة والتيسر في الإصدار 3.0.

ويعرض الجدول 1.I لمحة عن التغيرات بالمقارنة مع الإصدار 2.0.

**الجدول 1.I – التغيرات بين الإصدارين 2.0 و3.0 من نظام تحديد درجات لمواطن الضعف الشائعة**

| الإصدار 2.0 | الإصدار 3.0 |
|---|---|
| تحسب علامة مواطن الضعف بحسب التأثير الإجمالي على المنصة المضيفة. | تحسب علامة مواطن الضعف الآن بحسب التأثير على المكون المتأثر. |
| لا يتم التعرف إلى الحالات التي يؤثر فيها موطن ضعف يعتري تطبيقاً ما على التطبيقات الأخرى في النظام نفسه. | يشمل الآن مقياس جديد هو "النطاق" مواطن الضعف في الحالات التي يكون فيها *الشيء الذي تعرض للتأثير* (المكون المتأثر) مختلفاً عن *الشيء الضعيف* (المكون الضعيف). |
| قد يخلط متجه النفاذ بين الهجمات التي تستلزم نفاذاً إلى النظام المحلي والهجمات على المعدات التي تستلزم وجوداً مادياً. | يتم الآن فصل القيم المحلية عن القيم المادية في مقياس متجه الهجوم. |
| في بعض الحالات، كان تعقيد النفاذ يخلط بين تشكيلة النظام وتفاعل المستخدم. | انقسم هذا المقياس إلى قسمين هما تعقيد الهجوم (المتعلق بتعقيد النظام) وتفاعل المستخدم (المتعلق بمشاركة المستخدم في هجوم ناجح). |
| كانت علامات مقياس الاستيقان تنحاز عملياً لناتجَيْن من النواتج الثلاثة الممكنة، فلا تستخلص بالفعل الطابع المتوخى من موطن الضعف. | يحل مقياس جديد هو "الامتيازات المطلوبة" محل الاستيقان، ويعكس الآن الامتيازات القصوى التي ينبغي أن يتمتع بها المهاجم، بدل عدد المرات التي يجب الاستيقان من هويته. |
| كانت مقاييس التأثير تعكس النسبة المئوية للتأثير الذي تعرض له تطبيق ضعيف. | تعكس قيم مقاييس التأثير الآن درجة التأثير وتُترجَم إلى قيم توصف على أنها "معدومة" أو "منخفضة" أو "مرتفعة". |
| لم تُعتبر المقاييس البيئية لتوزع الأهداف والأضرار الجانبية المحتملة مفيدة. | استعيض عن توزع الأهداف والأضرار الجانبية المحتملة بالعوامل المخففة. |
| لم يتمكن هذا الإصدار من التكيف لوضع علامة لعدة مواطن ضعف مستخدمة في هجوم واحد. | مع أن التوجيه في مجال وضع علامة لعدة مواطن ضعف ليس مقياساً رسمياً، إلا أنه موفَّر مع الاستغلال المتسلسل لمواطن الضعف. |
| لم توفّر أي مبادئ توجيهية لوضع علامات نوعية رسمية. | رُبطت النطاقات الرقمية بتصنيف نوعي مؤلف من خمس نقاط. |

## 3.I دليل لوضع العلامات

يقدَّم فيما يلي عدد من المقترحات الموجّهة إلى المحللين عند وضع علامات لمواطن الضعف بواسطة الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

### 1.3.I وضع علامة بواسطة نظام تحديد درجات لمواطن الضعف الشائعة في دورة حياة الاستغلال

عندما يعي المحللون متى ينبغي وضع علامة لآثار مواطن الضعف، ينبغي أن يحصروا هذه الآثار في الأثر النهائي المعقول الذي سيتمكن المهاجم حتماً من تحقيقه في رأيهم. وينبغي للعلامة الفرعية لإمكانية الاستغلال أن تتضمن القدرة على إحداث هذا الأثر كحد أدنى، ولكن يمكنها أن تشمل أيضاً تفاصيل مستقاة من وصف موطن الضعف. ولنأخذ على سبيل المثال موطني الضعف التاليين:

في موطن الضعف 1، يستطيع مهاجم بعيد لم تستيقن هويته أن يرسل طلباً مبتكراً عادياً إلى مخدم ويب يدفع المخدم إلى الإفصاح عن النص الكامل لكلمة السر العادية للحساب الجذري (للمسؤول). ولا يعرف المحلل سوى من مقاييس العلامة الفرعية لإمكانية الاستغلال ومن وضعف موطن الضعف أن المهاجم نفذ إلى النظام لإرسال طلب مبتكر إلى مخدم الويب من أجل استغلال موطن الضعف. ويُفترض أن يتوقف التأثير عند هذا الحد؛ وفي حين *قد* يتمكن المهاجم من استخدام هذه المعلومات كي ينفذ شفرة في وقت لاحق منتحلاً صفة المسؤول، يُجهل أنه يحظى بدعوة إلى الدخول أو يعرف طريقة لتنفيذ أوامر بواسطة هذه المعلومات. ولا يشكل الحصول على كلمة السر هذه فقداناً مباشراً وخطيراً للسرية إلا في حال:

– Base score: 7.5 [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N]

وفي موطن الضعف 2، يستطيع مستخدم محلي له امتيازات قليلة أن يرسل طلباً مبتكراً عادياً إلى نظام التشغيل يدفعه إلى الإفصاح عن النص الكامل لكلمة السر العادية للحساب الجذري (للمسؤول). ويعرف المحلل من مقاييس العلامة الفرعية لإمكانية الاستغلال ومن موطن الضعف أن المهاجم يمكن أن ينفذ إلى نظام التشغيل ويدخل كمهاجم محلي قليل الامتيازات. ويشكل الحصول على كلمة السر هذه فقداناً مباشراً وخطيراً للسرية والحصانة والتيسر لأن المحلل يمكنه أن يصدر على نحو معقول أوامر باعتباره الحساب الجذري/حساب المسؤول (على افتراض أن المهاجم يمكنه أن يخرج من حسابه الخاص ويدخل مجدداً من الحساب الجذري):

– Base score: 7.8 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H]

### 2.3.I السرية والحصانة مقابل التأثير على التيسر

تشير مقاييس السرية والحصانة إلى الآثار التي تؤثر على *البيانات* التي تستعملها هذه الخدمة، مثل مضامين الويب التي جرى تغييرها بسوء نية أو ملفات النظام التي سُرقت. ويشير مقياس التأثير على التيسر إلى *تشغيل* الخدمة. وهذا يعني أن مقياس التيسر يعبّر عن أداء الخدمة نفسها وتشغيلها – وليس عن تيسر البيانات. ولنأخذ على سبيل المثال موطن ضعف في خدمة إنترنت مثل الويب أو البريد الإلكتروني أو نظام أسماء الميادين (DNS) يسمح لمهاجم بأن يغير أو يحذف جميع ملفات الويب في دليل، فهذا سيؤثر على الحصانة أكثر من التيسر. والسبب في ذلك هو أن خدمة الويب ما زالت تعمل بشكل سليم – إلا أنها تنتج مضامين متغيرة.

### 3.3.I استغلال مواطن ضعف محلية على يد مهاجمين بعيدين

في الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة، يشير الإرشاد 5 لحساب العلامات إلى ما يلي: "عندما يمكن استغلال موطن ضعف محلياً ومن الشبكة على السواء، ينبغي اختيار قيمة "الشبكة". وعندما يمكن استغلال موطن ضعف محلياً ومن الشبكات المجاورة على السواء، ولكن ليس من الشبكات البعيدة، ينبغي اختيار قيمة "شبكة مجاورة". وعندما يمكن استغلال موطن ضعف من الشبكات المجاورة والشبكات البعيدة، ينبغي اختيار قيمة "شبكة". وأدى هذا الإرشاد في بعض الأحيان إلى لبس في الحالات التي يحتال فيها المهاجم على مستخدم كي يقوم بتنزيل وثيقة مشوهة من مخدم ويب بعيد، مستغلاً بذلك موطن ضعف

في تحليل الملفات. وفي هذه الحالة، يعتبر المحللون الذين يستخدمون الإصدار 2.0 أن مواطن الضعف هذه هي "شبكة"، منتجين علامات بسلسلتي المقاييس التاليتين:

- AV:N/AC:M/Au:N/C:P/I:P/A:P أو AV:N/AC:M/Au:N/C:C/I:C/A:C

وجرى تحسين هذا التوجيه في الإصدار 3.0 بتوضيح معنى قيمتي الشبكة والشبكة المجاورة لمقياس متجه الهجوم. وبوجه خاص، ينبغي للمحللين ألا يضعوا علامة للشبكة أو الشبكة المجاورة إلا إذا كان موطن الضعف مسنداً إلى كدسة الشبكة. أما مواطن الضعف التي تتطلب تفاعل المستخدم الذي يقوم بتنزيل أو تلقي مضمون ضارّ (يمكن أن يُنقل أيضاً محلياً عن طريق محرّكات الناقل التسلسلي الشامل مثلاً)، فينبغي أن توضع لها علامة قيمتها "محلية".

وعلى سبيل المثال، فإن موطن ضعف في تحليل الوثائق لا يتم استغلاله بالاعتماد على الشبكة، ينبغي عادةً أن يحظى بعلامة قيمتها "محلية"، بصرف النظر عن الطريقة المستخدمة لتوزيع هذه الوثيقة الضارة (فمثلاً، يمكن أن يكون ذلك عبر رابط يؤدي إلى موقع في الويب أو عن طريق مفتاح لناقل تسلسلي شامل).

### 4.3.I مواطن الضعف في البرمجة العابرة للموقع

في الإصدار 2.0 من نظام تحديد درجات لمواطن الضعف الشائعة، كان لا بدّ من توفير توجيه معيّن لإنتاج علامات أعلى من الصفر لمواطن الضعف في البرمجة العابرة للموقع (XSS)، لأن علامات مواطن الضعف كانت تُحسب نسبة إلى نظام التشغيل المضيف الذي يحتوي موطن الضعف. وكان موطن الضعف العادي في البرمجة العابرة للموقع ينتج علامة تصف قيمتها تأثيراً جزئياً على الحصانة نتيجة تغير ردّ مخدم الويب على الزبون: AV:N/AC:M/Au:N/C:N/I:P/A:N. واستمرّ ذلك حتى لمواطن ضعف البرمجة العابرة للموقع القائمة على نموذج موضوع وثائقي (DOM)، فمع أن مواطن الضعف هذه قد تنشأ عن التفاعل مع المخدم فإنها تُستغل بالكامل في حاسوب الزبون (مثلاً عندما تحلل لغة "JavaScript" التي يوفرها المخدم سلسلة الطلب التي أُرسلت إلى المخدم).

وهذا السيناريو هو من السيناريوهات الرئيسية التي صُمم من أجلها "النطاق" – والتي لا يتعرض فيها المكون الضعيف لأي أثر (مثل مخدم ويب أو لغة "JavaScript" التي يوفرها مخدم الويب) وإنما مكون تدار امتيازاته على يد سلطة مستقلة (مثل بيئة متصفح الزبون). ومن هنا، ففي إطار الإصدار 3.0، لا حاجة إلى حصر مواطن ضعف البرمجة العابرة للموقع في الآثار المحدودة أو المعدومة التي يتعرض لها المخدم، وبات من الممكن حساب علامتها بالنظر إلى الآثار التي تعرّض لها الزبون. وقد تُحسب علامة موطن الضعف في البرمجة العابرة للموقع المنعكسة، الذي سمح لمهاجم بإعطاء رابط مضرّ للضحية وتنفيذ لغة "JavaScript" في متصفحها على النحو التالي:

- CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

### 5.3.I الاعتراض الوسيط

يسمح الإصدار 3.0 اليوم صراحة بوضع علامة لهجمات الاعتراض الوسيط. ففي حين لا يتطرق الإصدار 2.0 بوجه محدد إلى هذا الأمر، يتم في الإصدار 3.0 معالجة هذا النوع من الهجمات في إطار مقياس تعقيد الهجوم.

### 6.3.I مواطن الضعف في المعدات

بالإضافة إلى ذلك، وفي حين صُمّم نظام تحديد درجات لمواطن الضعف الشائعة، بشكل رئيسي، من أجل وضع علامة لمواطن الضعف في البرمجيات والآثار عليها، فإن الإصدار 3.0 مجهز الآن بشكل أفضل لوضع علامة أيضاً على الآثار التي تشمل مكونات المعدات والآثار الشبكية.

### 7.3.I تسلسل استغلال مواطن الضعف

صُمم نظام تحديد درجات لمواطن الضعف الشائعة من أجل ترتيب وتصنيف كل موطن من مواطن الضعف. ولكن من المهم دعم احتياجات الأوساط المعنية بتحليل مواطن الضعف، من خلال معالجة الأوضاع التي تُستغل فيها عدة مواطن ضعف أثناء هجوم واحد هدفه تعطيل نظام مضيف أو تطبيق. وتسمى عملية وضع علامة لعدة مواطن ضعف بهذا الشكل "تسلسل استغلال مواطن الضعف". وجدير بالذكر أن هذه العملية ليست مقياساً رسمياً، وإنما تُجرى لتوجيه المحللين أثناء حساب علامة هذا النوع من الهجمات.

وعند حساب علامة إحدى سلاسل مواطن ضعف، تقع على المحلل مسؤولية تحديد مواطن الضعف المترابطة التي تشكل علامة السلسلة. وينبغي للمحلل أن يحصي مواطن الضعف المختلفة وعلاماتها فضلاً عن علامة السلسلة. وقد يتم مثلاً الإفصاح عن ذلك في مذكرة تكشف النقاب عن مواطن الضعف وتُنشر في صفحة ويب.

وفضلاً عن ذلك، قد يُدرج المحلل أنواعاً أخرى من مواطن الضعف ذات الصلة التي يمكن ربطها بسلسلة مواطن الضعف التي حُسبت علامتها. وعلى وجه الخصوص، يمكن أن يحصي المحلل أنواعاً (أو فئات) عامة لمواطن الضعف ذات الصلة التي تُربط عادة ببعضها، أو أن يوفّر معلومات إضافية عن الشروط المسبقة المطلوبة التي يجب استيفاؤها. وعلى سبيل المثال، قد يصف المحلل كيف تنذر بعض أنواع مواطن الضعف في حقن لغة الاستعلام البِنْيَوية (SQL) بهجوم على البرمجة العابرة للموقع، أو كيف يمنح نوع معين من فيض الذاكرة امتيازات محلية. ويؤدي تحديد الأنواع أو الفئات العامة لمواطن الضعف إلى توفير حد أدنى من المعلومات اللازمة لتحذير المستخدمين الآخرين دون وجود احتمال لفتح أعين المهاجمين على فرص استغلال جديدة.

ومن جهة أخرى، قد يحدد المحلل (في شكل قائمة يسهل قراءتها وفهمها لمواطن الضعف مثل معرفات (ID) مواطن الضعف والتعرّض الشائعة (CVE) أو تعداد مواطن الضعف الشائعة (CWE)) قائمة مستوفاة بمواطن الضعف المحددة ذات الصلة التي يُعرف (أو يُرجح) أنها ترتبط بسلسلة واحدة أو أكثر من مواطن الضعف المترابطة التي تُسند إليها علامة من أجل استغلال نظام لتكنولوجيا المعلومات. وإذا لم يكن من الممكن استغلال موطن ضعف ما إلا بعد استيفاء شروط مسبقة أخرى (مثل استغلال موطن ضعف آخر أولاً)، فإنه من المقبول أن تُمزج علامتان أو أكثر من علامات نظام تحديد درجات لمواطن الضعف الشائعة بغية وصف سلسلة مواطن الضعف من خلال حساب علامة من أجل المقاييس الأقل تقييداً لحساب العلامة الفرعية لإمكانية الاستغلال، ومن خلال حساب علامة المقاييس الأكثر تأثيراً لحساب العلامة الفرعية للتأثير. وفيما يلي أمثلة تستخدم العلامات الفرعية لإمكانية الاستغلال والنطاق والتأثير لوصف السلسلة:

موطن الضعف A هو: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H، وعلى النحو المبين في المتجه، يجب أن يكون المستخدم مستخدماً محلياً قليل الامتيازات للتمكن من استغلاله. أما موطن الضعف B فهو: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L، ويمنح مهاجماً بعيداً دون امتيازات القدرة على تنفيذ شفرة في نظام مع إحداث آثار طفيفة إذا كان هناك مستخدم محلي يتفاعل لإتمام الهجوم. ومن هنا، وبالنظر إلى موطني الضعف A وB، يمكن وصف السلسلة C بأنها السلسلة B -> A: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H التي تدمج إمكانية استغلال B، ويبقى النطاق كما هو في الحالتين فضلاً عن تأثير A، لأنه إذا تمكن أحدهم من أن يستغل B ويحصل منه على تنفيذ الشفرة كمستخدم محلي، فإنه يكون قد استوفى الشروط المسبقة اللازمة للتمكن عندئذ من إطلاق A محدثاً أثراً من موطن الضعف A.

## 4.I مسرد مصطلحات

**سلطة:** حاوية حاسوبية لمنح الامتيازات إلى الموارد وإدارتها. ومن الأمثلة على هذه السلطات، تطبيق لقاعدة بيانات ونظام تشغيل وبيئة افتراضية.

**علامة سلسلة:** العلامة القاعدية التي تنتج عن حساب علامة موطنين أو أكثر من مواطن الضعف المترابطة.

**الاستغلال المتسلسل لمواطن ضعف:** انظر تسلسل استغلال مواطن الضعف.

**مكون:** يشير إلى مكون برمجية أو معدة.

**مكون برمجية**: برنامج برمجي أو وحدة برمجية تتضمن تعليمات حاسوبية ينبغي تنفيذها. ومن الأمثلة على ذلك، نظام تشغيل أو تطبيق للإنترنت أو محرّك جهاز.

**مكون معدة**: جهاز حاسوبي مادي.

**مكون متأثر**: المكون (أو المكونات) الذي عانى (التي عانت) من التبعات الناجمة عن موطن الضعف المستغل. ويمكن أن يكون المكون الضعيف نفسه، أو أن يكون مختلفاً عنه إذا طرأ تغيير في النطاق.

**امتيازات**: مجموعة من الحقوق (وهي عادة القراءة والكتابة والتنفيذ) الممنوحة لمستخدم أو لعملية يجريها المستخدم، والتي تحدد النفاذ إلى الموارد الحاسوبية.

**موارد**: جسم برمجي أو شبكي يمكن الوصول إليه أو تغييره أو استهلاكه بواسطة جهاز حاسوبي. ومن الأمثلة على ذلك، ملفات الحاسوب أو الذاكرة أو دورات وحدة المعالجة المركزية أو النطاق العريض الشبكي.

**نطاق**: مجموعة من الامتيازات التي تحددها وتديرها سلطة تخويل عند السماح بالنفاذ إلى الموارد الحاسوبية.

**موطن ضعف**: ضعف أو عيب في مكون برمجية (أو معدة).

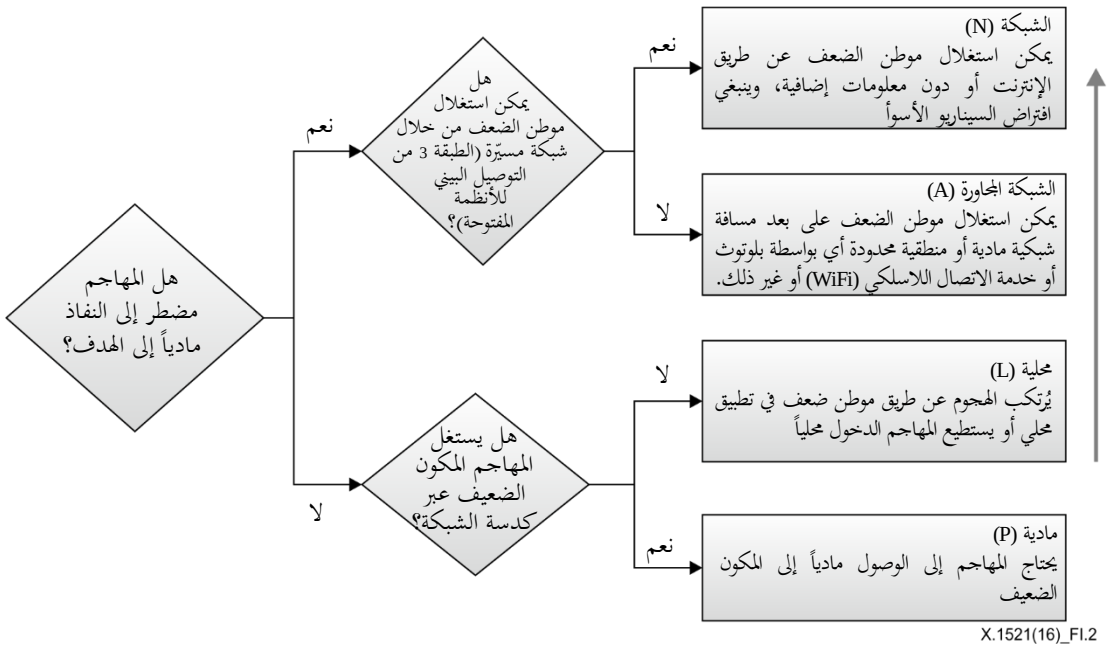
**تسلسل استغلال مواطن الضعف**: الاستغلال المتتابع لعدة مواطن ضعف بغية الهجوم على نظام لتكنولوجيا المعلومات، حيث تتطلب عملية استغلال واحدة أو أكثر في نهاية السلسلة إتمام عمليات استغلال سابقة بنجاح لتحقيق الاستغلال. وانظر أيضاً التعريف المتاح من خلال الرابط http://cwe.mitre.org/documents/glossary/#Chain.

**مكون ضعيف**: مكون برمجية (أو معدة) يشكو من ضعف وينبغي إصلاحه.

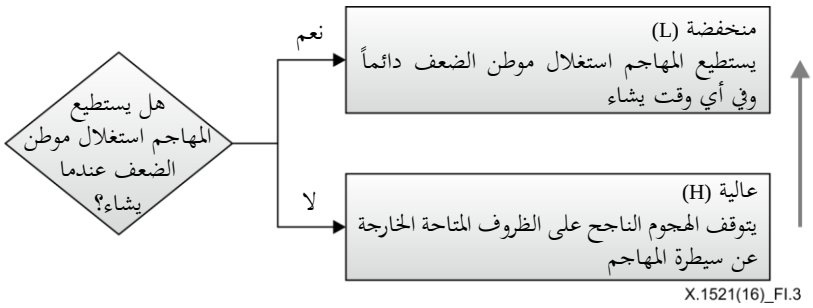
## 5.I جزء عن وضع العلامات

يعرض الجزء الخاص بوضع العلامات لمحة سريعة عن حساب علامات مواطن الضعف في الإصدار 3.0. والغرض منه هو تكملة البحث الوارد في وثيقة المواصفات بشأن وضع العلامات.

### 1.5.I متجه الهجوم

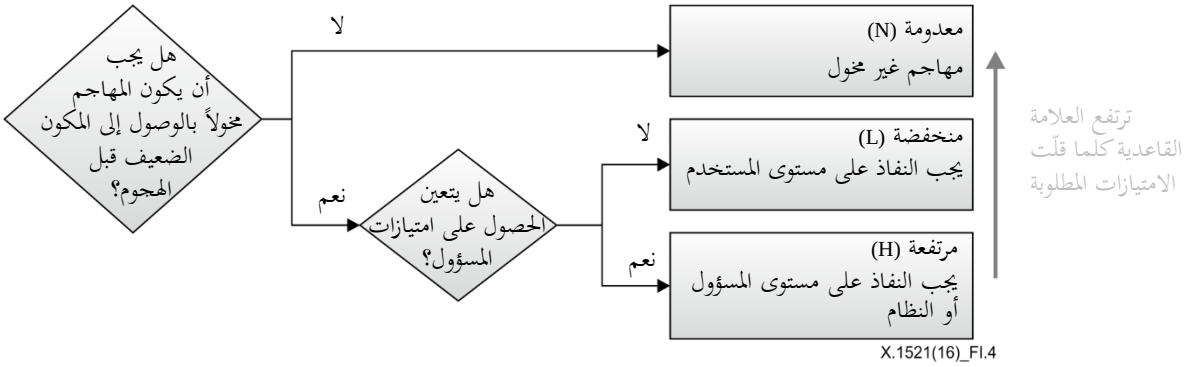


### 2.5.I تعقيد الهجوم

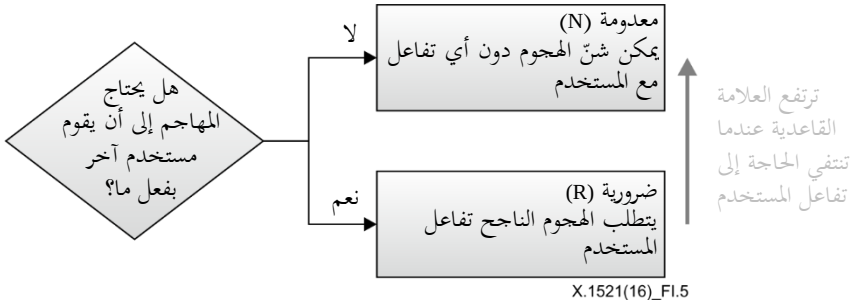



**ملاحظة:** يُستثنى من ذلك تفاعل المستخدم

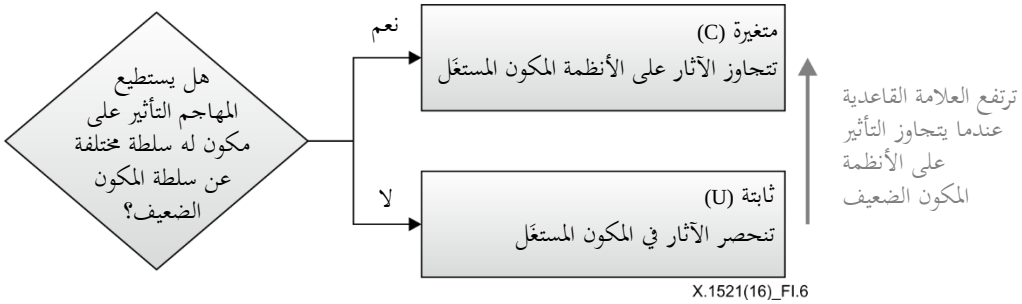
### 3.5.I الامتيازات المطلوبة




### 4.5.I تفاعل المستخدم

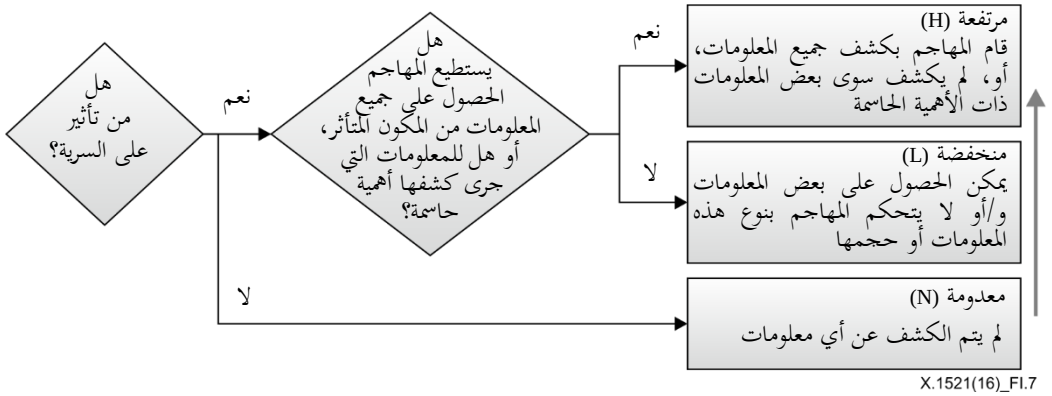



### 5.5.I النطاق



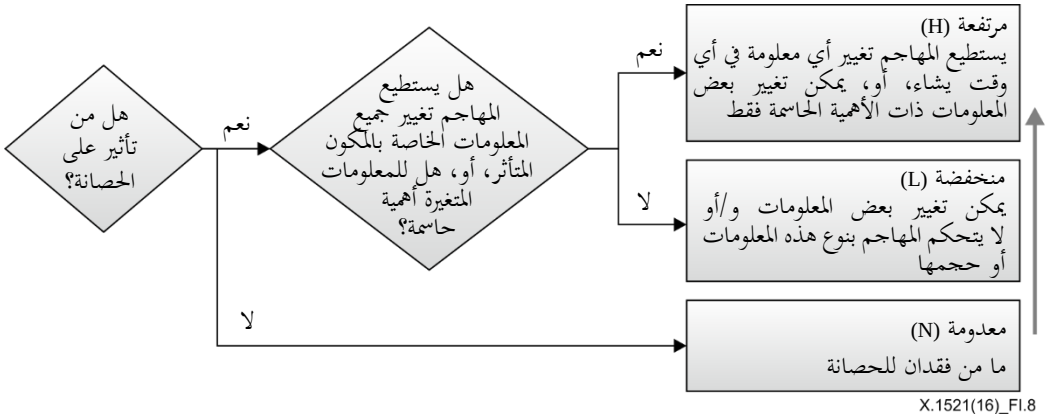

**ملاحظة:** إذا لم يطرأ أي تغيير على النطاق، تعكس الآثار على السرية والحصانة والتيسر التبعات على المكون الضعيف، وإلا تعكس التبعات على المكون الذي تعرّض للأثر الأكبر.

### 6.5.I التأثير على السرية



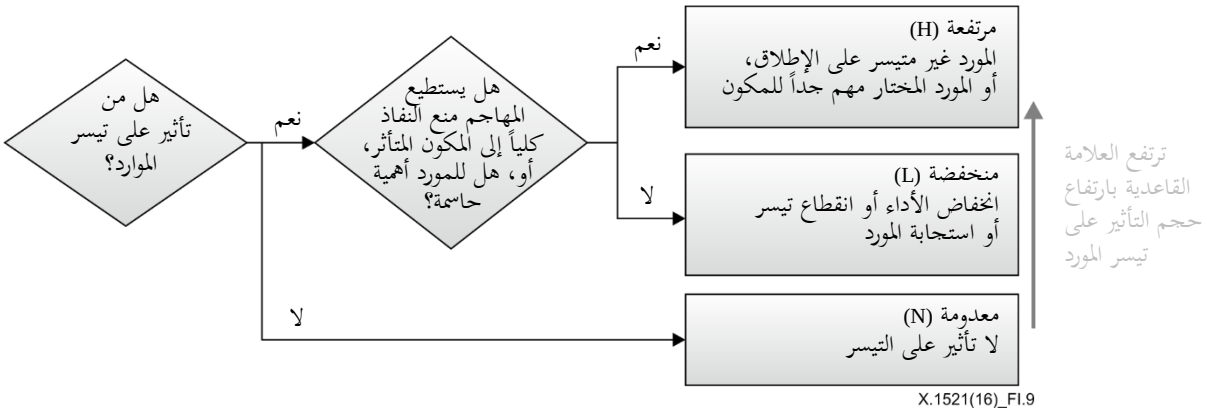

X.1521(16)_FI.7

### 7.5.I التأثير على الحصانة




X.1521(16)_FI.8

### 8.5.I التأثير على التيسر




X.1521(16)_FI.9

# التذييل II

# الموارد والروابط

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

فيما يلي مراجع مفيدة لوثائق إضافية عن الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة.

| المورد | الموقع |
|---|---|
| وثيقة المواصفات | تتضمن وصفاً للمقاييس ومعادلات وسلسلة متجهات، وهي متاحة في العنوان التالي: http://www.first.org/cvss/specification-document |
| دليل للمستخدمين | يتضمن بحثاً إضافياً عن الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، وجزءاً عن وضع العلامات، ومسرداً، وهو متاح في العنوان التالي: http://www.first.org/cvss/user-guide |
| وثيقة أمثلة | تتضمن أمثلة عملية عن كيفية وضع العلامات في الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، وهي متاحة في العنوان التالي: https://www.first.org/cvss/examples |
| شعار الإصدار 3.0 | صور منخفضة وعالية الاستبانة متاحة في العنوان التالي: http://www.first.org/cvss/identity |
| العمليات الحسابية الخاصة بالإصدار 3.0 | التنفيذ المرجعي لمعادلات الإصدار 3.0 من نظام تحديد درجات لمواطن الضعف الشائعة، وهي متاحة في العنوان التالي: http://www.first.org/cvss/calculator/3.0 |
| مخطط لغة الوسم القابلة للتوسيع XML | تعريف المخطط متاح في العنوان التالي: https://www.first.org/cvss/cvss-v3.0.xsd |

# بيبليوغرافيا


[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange*

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2011), *Common weakness enumeration.*

## سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

| | |
|---|---|
| السلسلة A | تنظيم العمل في قطاع تقييس الاتصالات |
| السلسلة D | المبادئ العامة للتعريفة |
| السلسلة E | التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية |
| السلسلة F | خدمات الاتصالات غير الهاتفية |
| السلسلة G | أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية |
| السلسلة H | الأنظمة السمعية المرئية والأنظمة متعددة الوسائط |
| السلسلة I | الشبكة الرقمية متكاملة الخدمات |
| السلسلة J | الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط |
| السلسلة K | الحماية من التداخلات |
| السلسلة L | البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها |
| السلسلة M | إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات |
| السلسلة N | الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية |
| السلسلة O | مواصفات تجهيزات القياس |
| السلسلة P | المطاريف وطرائق التقييم الذاتية والموضوعية |
| السلسلة Q | التبديل والتشوير |
| السلسلة R | الإرسال البرقي |
| السلسلة S | التجهيزات المطرافية للخدمات البرقية |
| السلسلة T | المطاريف الخاصة بالخدمات التليماتية |
| السلسلة U | التبديل البرقي |
| السلسلة V | اتصالات البيانات على الشبكة الهاتفية |
| **السلسلة X** | **شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن** |
| السلسلة Y | البنية التحتية العالمية للمعلومات وجوانب بروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية |
| السلسلة Z | اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات |

طُبعت في سويسرا
جنيف، 2017