ITU-T CYBEX standards for cybersecurity information dissemination and exchange

ITU-ATU Workshop on Cybersecurity Strategy in African Countries

Session 4: National versus regional versus international

Martin Euchner
Adviser, ITU-T

Khartoum, Sudan, 24-26 July 2016

(See notes pages for more information)

Contents

- ITU-T Study Group 17, and Question 4/17, Cybersecurity
- Cyberspace security, ITU-T definition of Cybersecurity

- Knowledge-based standards for CYbersecurity Information eXchange (CYBEX) (ITU-T X.1500-series Recommendations)
  - CVE: Common Vulnerability Enumeration
  - CVSS: Common Vulnerability Scoring System (3.0)
  - Common Weakness Enumeration (CWE)
  - Common weakness scoring system (CWSS)
  - Language for the open definition of vulnerabilities and for the assessment of a system state (OVAL)
  - Discovery mechanisms in the exchange of cybersecurity information
  - Incident object description exchange format (IODEF)
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Malware attribute enumeration and classification (MAEC)

ITU-T Study Group 17 mandate

- Title: Security

  Responsible for building confidence and security in the use of information and communication technologies (ICTs).

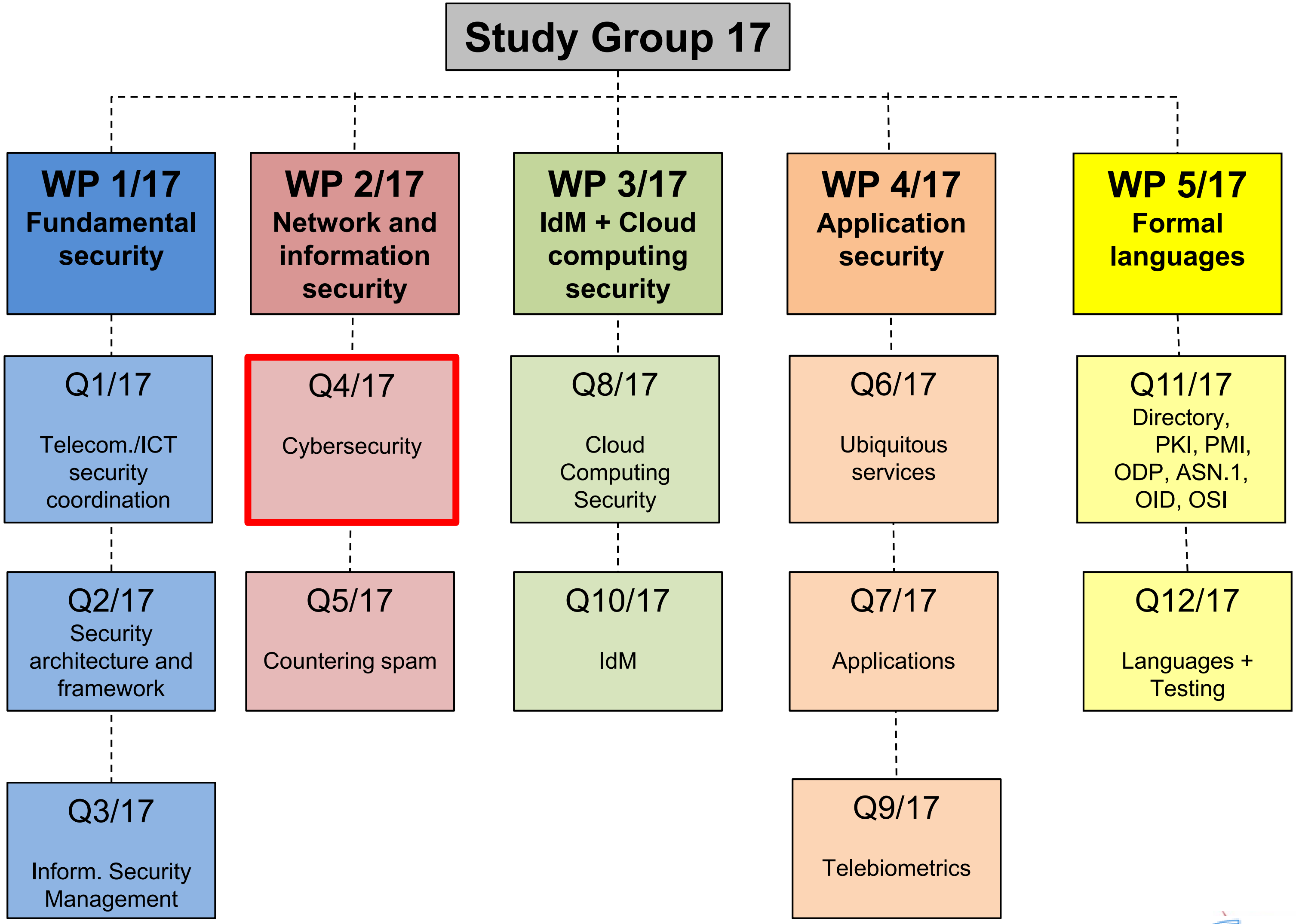
  This includes studies relating to **cybersecurity**, **security management**, **countering spam** and **identity management**.

  It also includes security architecture and framework, protection of personally identifiable information, and security of applications and services for the Internet of things, smart grid, smartphone, IPTV, web services, social network, cloud computing, mobile financial system and telebiometrics.

  Also responsible for the application of open system communications including directory and object identifiers, and for technical languages, the method for their usage and other issues related to the software aspects of telecommunication systems, and for conformance testing to improve quality of Recommendations.

  Chairman: Arkadiy Kremer, Russian Federation

ITU-T SG17, Security



Study Group 17

WP 1/17
Fundamental security

Q1/17
Telecom./ICT security coordination

Q2/17
Security architecture and framework

Q3/17
Inform. Security Management

WP 2/17
Network and information security

Q4/17
Cybersecurity

Q5/17
Countering spam

WP 3/17
IdM + Cloud computing security

Q8/17
Cloud Computing Security

Q10/17
IdM

WP 4/17
Application security

Q6/17
Ubiquitous services

Q7/17
Applications

Q9/17
Telebiometrics

WP 5/17
Formal languages

Q11/17
Directory, PKI, PMI, ODP, ASN.1, OID, OSI

Q12/17
Languages + Testing

Question 4/17
Cybersecurity

- Cybersecurity by design no longer possible; a new paradigm:
  - know your weaknesses → minimize the vulnerabilities
  - know your attacks → share the heuristics within trust communities
- Current work program (6 Recommendations under development)
  - X.1500 suite: Cybersecurity Information Exchange (CYBEX) – non-prescriptive, extensible, complementary techniques for the new paradigm
    - Weakness, vulnerability and state
    - Event, incident, and heuristics
    - Information exchange policy
    - Identification, discovery, and query
    - Identity assurance
    - Exchange protocols
  - Non-CYBEX deliverables include compendiums and guidelines for
    - Abnormal traffic detection
    - Botnet mitigation
    - Attack source attribution (including traceback)
- Extensive relationships with many external bodies
- Rapporteur: Mr Youki KADOBAYASHI

Definition of Cybersecurity

- Definition of Cybersecurity
  (ref. Rec. ITU-T X.1205, Overview of cybersecurity):
  Cybersecurity is the collection of *tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*.
  Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
  Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.
  The general security objectives comprise the following:
  - Availability
  - Integrity, which may include authenticity and non-repudiation
  - Confidentiality.

Capacity building with ITU-T cybersecurity standards

- Existing process-oriented standards, as well as checklist standards, should be complemented with detailed knowledge-base of cybersecurity, because:
  - Cyber-risks are highly volatile
  - Chain reactions are typical
    difficult to estimate the risk without considering technical detail
  - You'll need to communicate the detail

- ITU-T provides knowledge-base standards.

Improving cybersecurity throughout IT infrastructure lifecycle

Development	Deployment	Assessment
CWE X.1524	CVE X.1520	OVAL X.1526
CAPEC X.1544	CVSS X.1521	CPE X.1528

Knowledge bases, compatible products, informed communities and ITU-T Recommendations are already helping diverse organizations to protect their IT infrastructures and customers

Examples of CYBEX usage

- **National coordination centers for cybersecurity** make use of vulnerability information identifiers and scoring standards for public alerting purposes.

- **Incident response teams** efficiently keep track of vulnerabilities and attack patterns through a set of concise identifiers as predicated by CYBEX.

- **System administrators** assess presence of vulnerabilities using software tools that employ CYBEX.

- **Cloud computing and network service providers** keep track of vulnerabilities in their infrastructure, where they are prioritized according to impact, using the standardized scoring method.

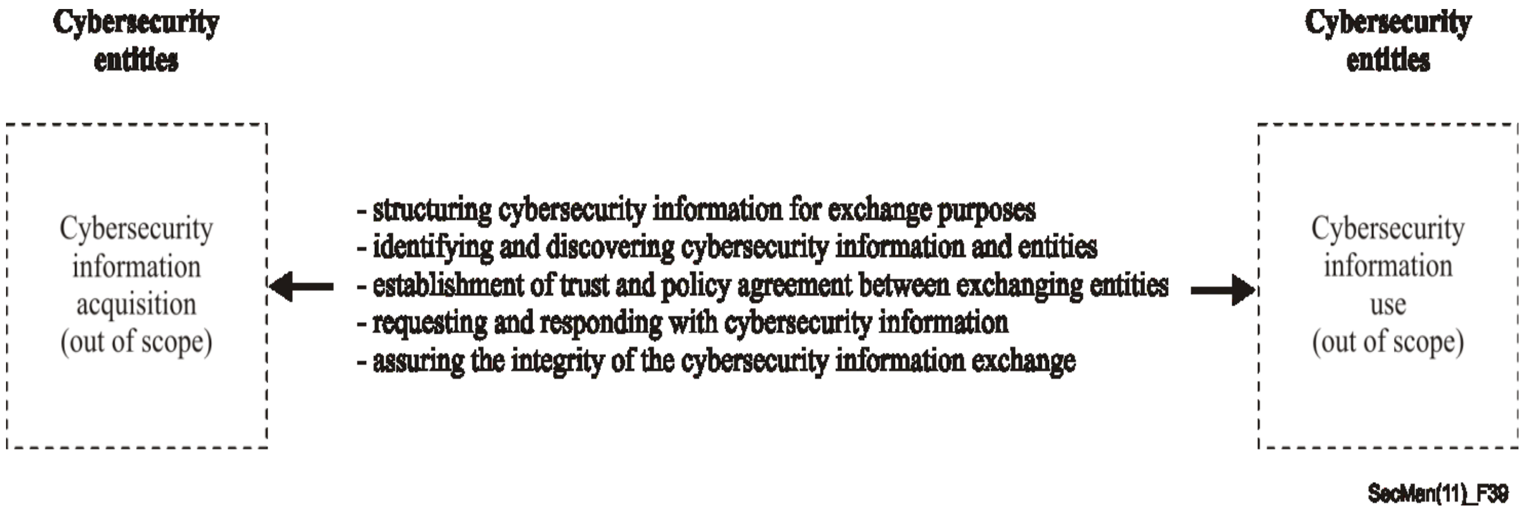
- **Embedded and IoT product developers** learn typical patterns of software weaknesses through public knowledge base that is also part of CYBEX.

- **Vulnerability researchers** collectively maintain knowledge bases of vulnerabilities, each of which can be linked and integrated through common vulnerability identifiers.

CYBERSECURITY INFORMATION EXCHANGE (CYBEX)

- Overview of cybersecurity information exchange (Rec. ITU-T X.1500)

- Procedures for the registration of arcs under the object identifier arc for cybersecurity information exchange (Rec. ITU-T X.1500.1)


Cybersecurity entities
Cybersecurity information acquisition (out of scope)
- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- establishment of trust and policy agreement between exchanging entities
- requesting and responding with cybersecurity information
- assuring the integrity of the cybersecurity information exchange
Cybersecurity entities
Cybersecurity information use (out of scope)
SecMan(11)_F39

Rec. ITU-T X.1500 - CYBEX model

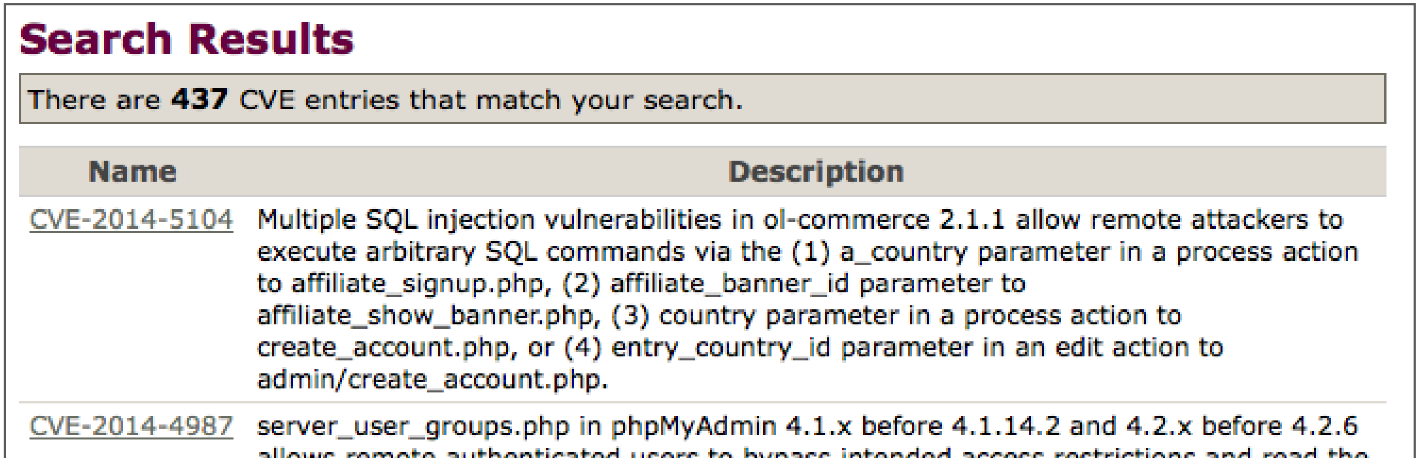
Knowledge base of vulnerabilities

CVE: Common Vulnerability Enumeration

- A structured means to exchange information on security vulnerabilities and exposures
- Provides a common identifier with status indicator, a brief description and references to related vulnerability report and advisories for publicly-known problems.
- Standardized as Rec. ITU-T X.1520
- Applicable to national vulnerability databases:
    - U.S. NIST NVD
    - Japan JVN

- CVE community: http://cve.mitre.org/
- R. Martin, “Managing Vulnerabilities in Networked Systems”, IEEE Computer, 34 (11), Nov 2001.

Example
Vulnerabilities of widely used software for data protection purposes

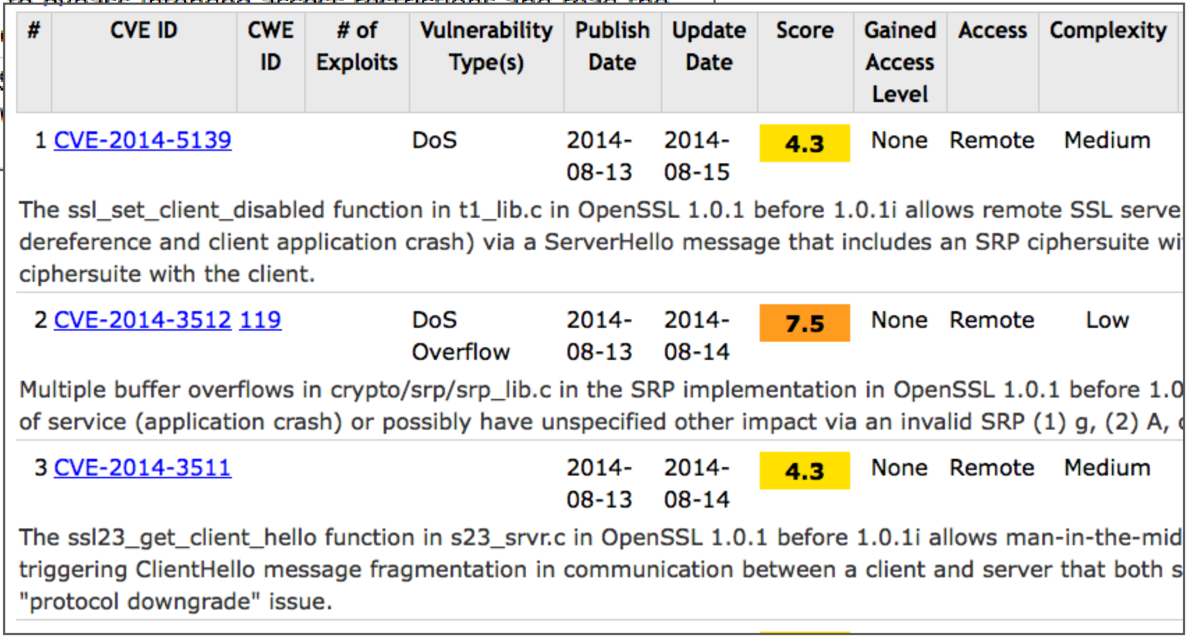


Search Results

There are **437** CVE entries that match your search.

Name	Description
CVE-2014-5104	Multiple SQL injection vulnerabilities in ol-commerce 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) a_country parameter in a process action to affiliate_signup.php, (2) affiliate_banner_id parameter to affiliate_show_banner.php, (3) country parameter in a process action to create_account.php, or (4) entry_country_id parameter in an edit action to admin/create_account.php.
CVE-2014-4987	server_user_groups.php in phpMyAdmin 4.1.x before 4.1.14.2 and 4.2.x before 4.2.6 allows remote authenticated users to bypass intended access restrictions and read the MySQL user list via a viewUsers re
CVE-2014-4260	Unspecified vulnerability in the My earlier, and 5.6.17 and earlier, allo and availability via vectors related

CVE entries for MySQL

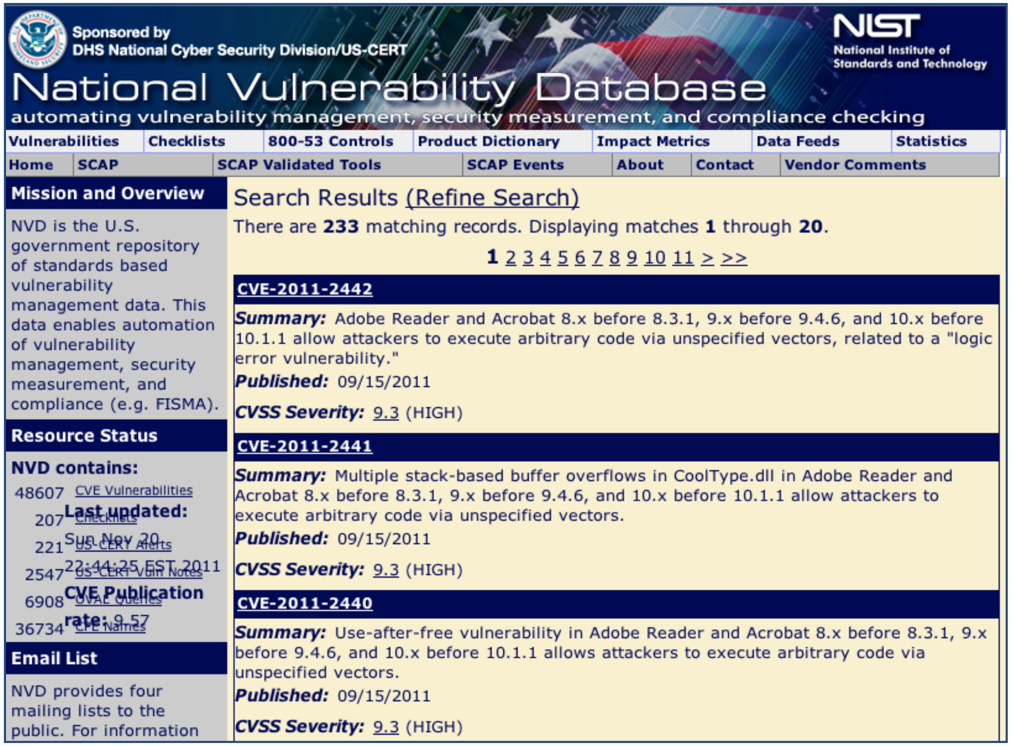


#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2014-5139			DoS	2014-08-13	2014-08-15	4.3	None	Remote	Medium
The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL serve dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite wi ciphersuite with the client.										
2	CVE-2014-3512	119		DoS Overflow	2014-08-13	2014-08-14	7.5	None	Remote	Low
Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0 of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A,										
3	CVE-2014-3511				2014-08-13	2014-08-14	4.3	None	Remote	Medium
The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-mid triggering ClientHello message fragmentation in communication between a client and server that both s "protocol downgrade" issue.										

CVE entries for OpenSSL

Ongoing proliferation of CVE

- More than 150 CVE-compatible products and services



Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

NIST
National Institute of Standards and Technology

Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics
Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

48607	CVE Vulnerabilities
207	Checklists
221	US-CERT Alerts
2547	US-CERT Vuln Notes
6908	OVAL Queries
36734	CPE Names

Last updated: Sun Nov 20 22:44:25 EST 2011

CVE Publication rate: 9.57

Email List

NVD provides four mailing lists to the public. For information

Search Results (Refine Search)

There are **233** matching records. Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 11 > >>

CVE-2011-2442

Summary: Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error vulnerability."

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

CVE-2011-2441

Summary: Multiple stack-based buffer overflows in CoolType.dll in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

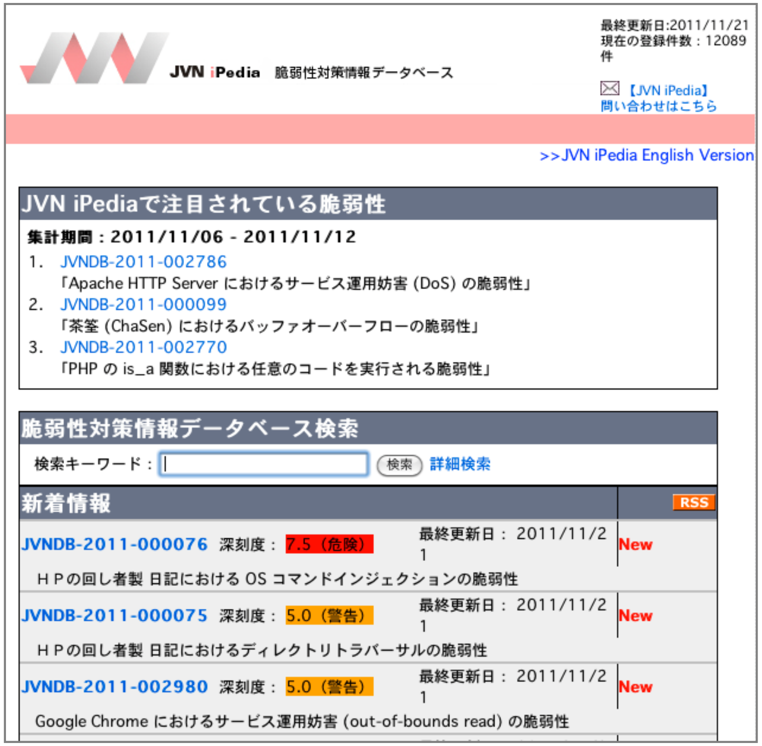
CVE-2011-2440

Summary: Use-after-free vulnerability in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.

Published: 09/15/2011

CVSS Severity: 9.3 (HIGH)

U.S.: NIST NVD



JVN iPedia　脆弱性対策情報データベース

最終更新日:2011/11/21
現在の登録件数：12089件

【JVN iPedia】
問い合わせはこちら

>>JVN iPedia English Version

JVN iPediaで注目されている脆弱性

集計期間：2011/11/06 - 2011/11/12

1. JVNDB-2011-002786
「Apache HTTP Server におけるサービス運用妨害 (DoS) の脆弱性」
2. JVNDB-2011-000099
「茶筌 (ChaSen) におけるバッファオーバーフローの脆弱性」
3. JVNDB-2011-002770
「PHP の is_a 関数における任意のコードを実行される脆弱性」

脆弱性対策情報データベース検索

検索キーワード：

新着情報

JVNDB-2011-000076 深刻度：7.5（危険） 最終更新日：2011/11/21 New
ＨＰの回し者製 日記における OS コマンドインジェクションの脆弱性

JVNDB-2011-000075 深刻度：5.0（警告） 最終更新日：2011/11/21 New
ＨＰの回し者製 日記におけるディレクトリトラバーサルの脆弱性

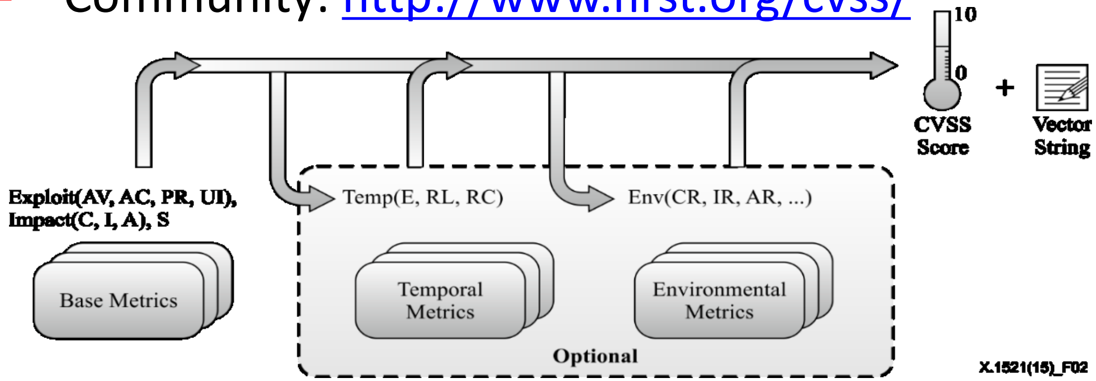
JVNDB-2011-002980 深刻度：5.0（警告） 最終更新日：2011/11/21 New
Google Chrome におけるサービス運用妨害 (out-of-bounds read) の脆弱性

Japan: IPA JVN

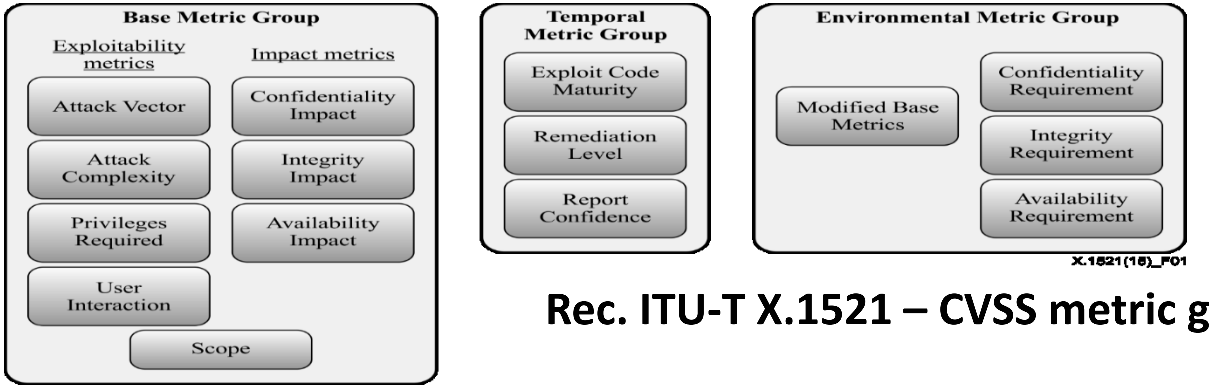
Quantification of vulnerabilities

facilitates prioritization during vulnerability management

- CVSS: Common Vulnerability Scoring System (3.0)
  - Base metrics: constant over time and across user environments
  - Temporal metrics: reflects vulnerability landscape
  - Environmental metrics: reflects user environments
  - Standardized as [Rec. ITU-T X.1521]
  - Community: [http://www.first.org/cvss/]



Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

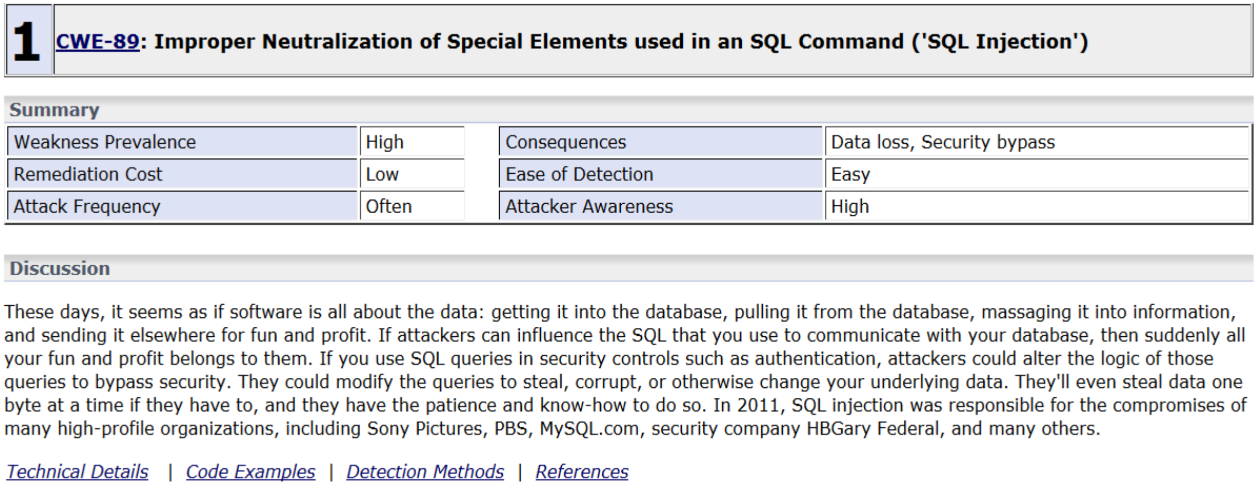


Rec. ITU-T X.1521 – CVSS metric groups

Taxonomy of vulnerabilities
Common Weakness Enumeration (CWE)

Rec. ITU-T X.1524

- Group same kind of vulnerabilities into a weakness, and give it a distinct number
- Provides common names for publicly known problems in the commercial or open source software
- Intended for security tools and services that can find weaknesses in source code and operational systems
- Helps better understand and manage software weaknesses related to architecture and design
- Community: http://cwe.mitre.org/



1 **CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

Summary

Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

Discussion

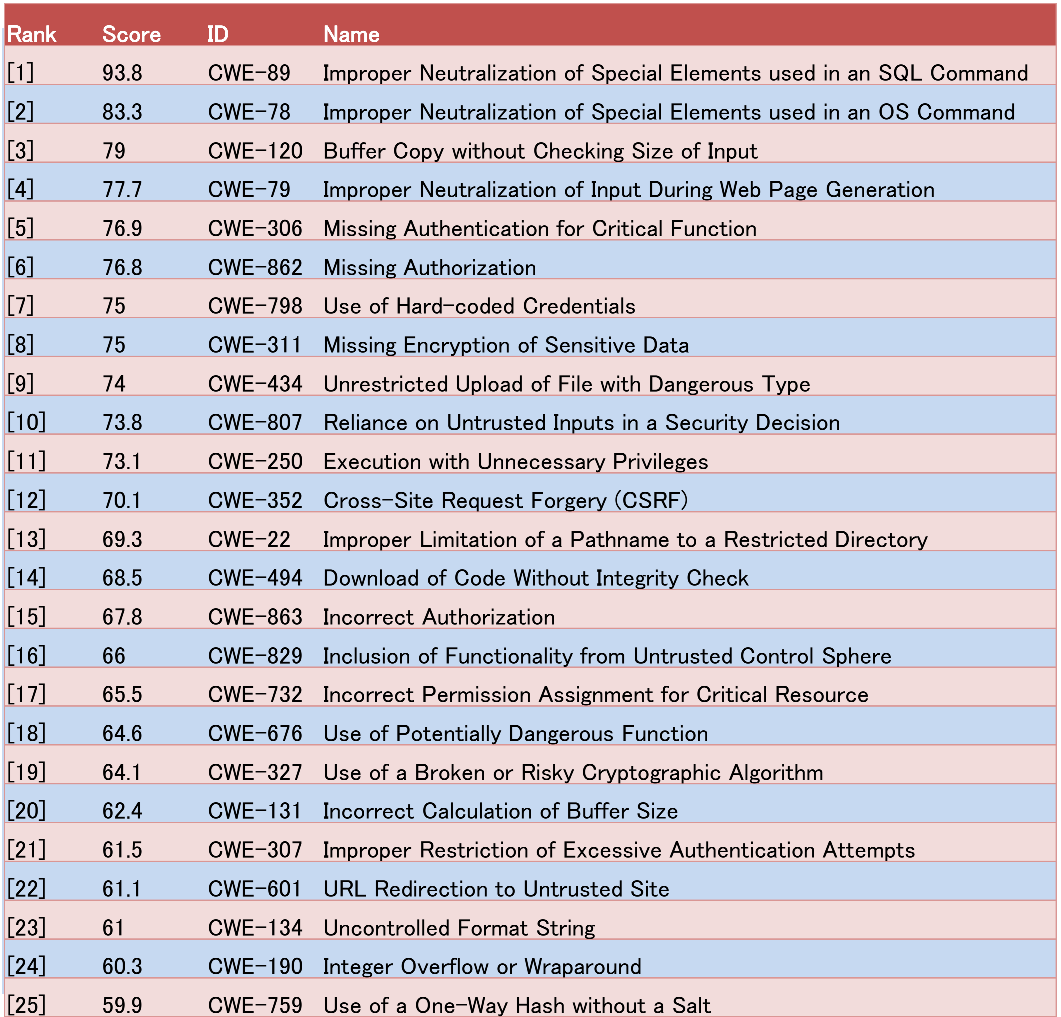
These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know-how to do so. In 2011, SQL injection was responsible for the compromises of many high-profile organizations, including Sony Pictures, PBS, MySQL.com, security company HBGary Federal, and many others.

Technical Details | *Code Examples* | *Detection Methods* | *References*

CWE top 25

http://cwe.mitre.org/top25/

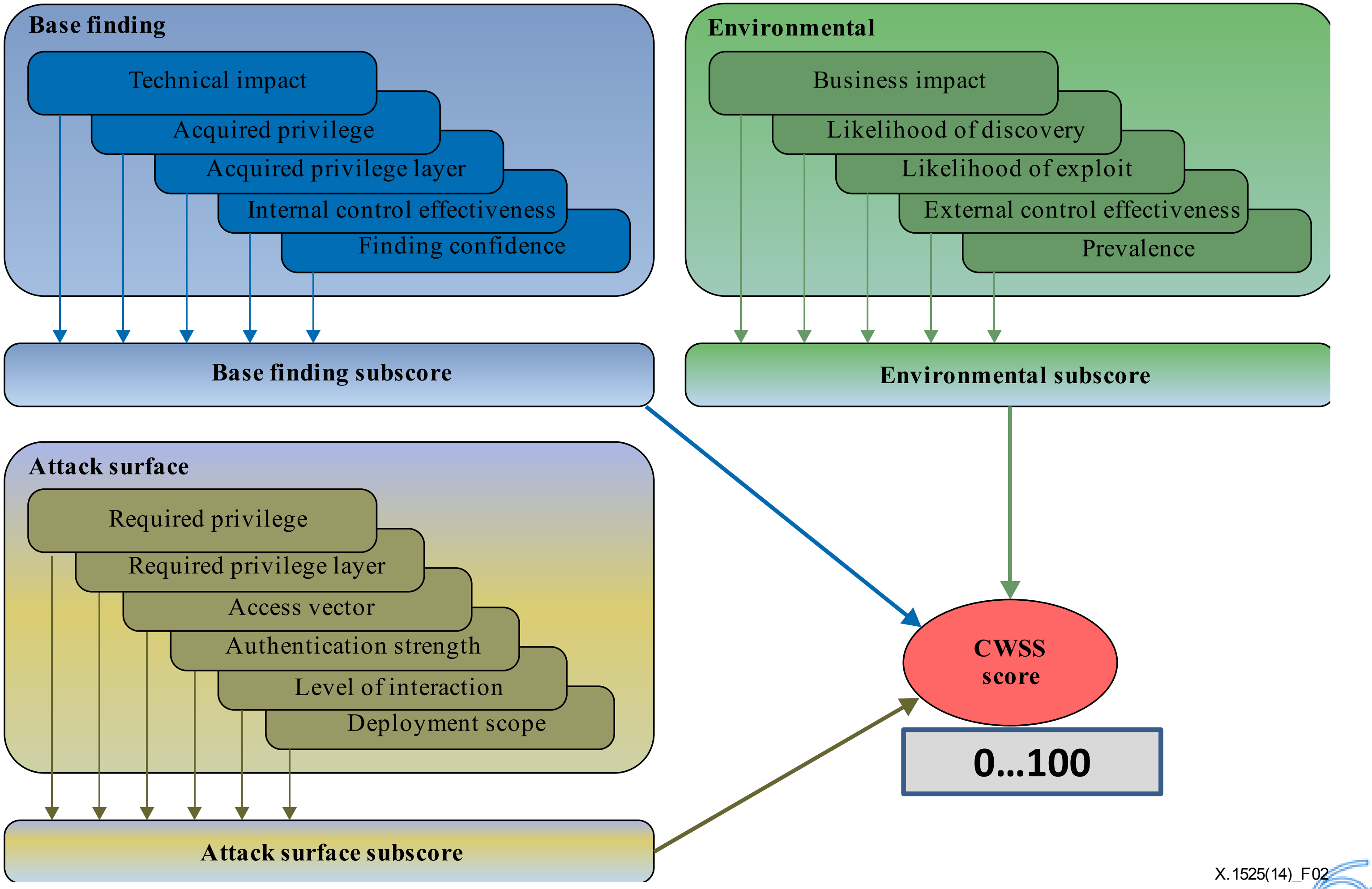
- Prioritized list of dangerous software errors
  - Intended to minimize software vulnerability and data breach
  - Any software for data protection needs serious consideration of these failure modes, among others
  - Useful for:
    - Procurement
    - Development, etc.



Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command
[3]	79	CWE-120	Buffer Copy without Checking Size of Input
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75	CWE-798	Use of Hard-coded Credentials
[8]	75	CWE-311	Missing Encryption of Sensitive Data
[9]	74	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site
[23]	61	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

CYBEX vulnerability/state exchange

- Common weakness scoring system (CWSS) (Rec. ITU-T X.1525)

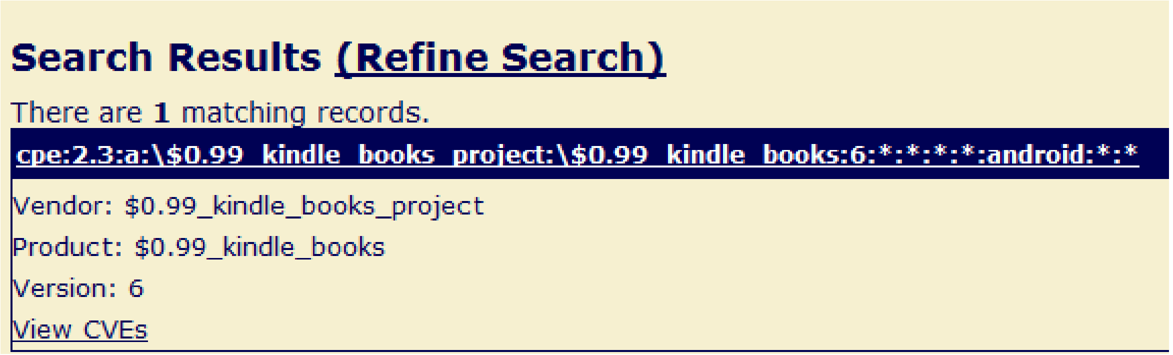


Rec. ITU-T X.1525 - CWSS scoring

Vulnerability assessment

- Language for the open definition of vulnerabilities and for the assessment of a system state (OVAL) (Rec. ITU-T X.1526)
  - A standard for assessment and reporting of machine state of computer systems; such as vulnerability state, patch state, configuration state.
  - OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.
  - Community: http://oval.mitre.org/

- Common platform enumeration (CPE) (Recs. ITU-T X.1528, X.1528.1, X.1528.2, X.1528.3, X.1528.4)



Search Results (Refine Search)

There are **1** matching records.

cpe:2.3:a:\$0.99_kindle_books_project:\$0.99_kindle_books:6:*:*:*:*:android:*:*

Vendor: $0.99_kindle_books_project

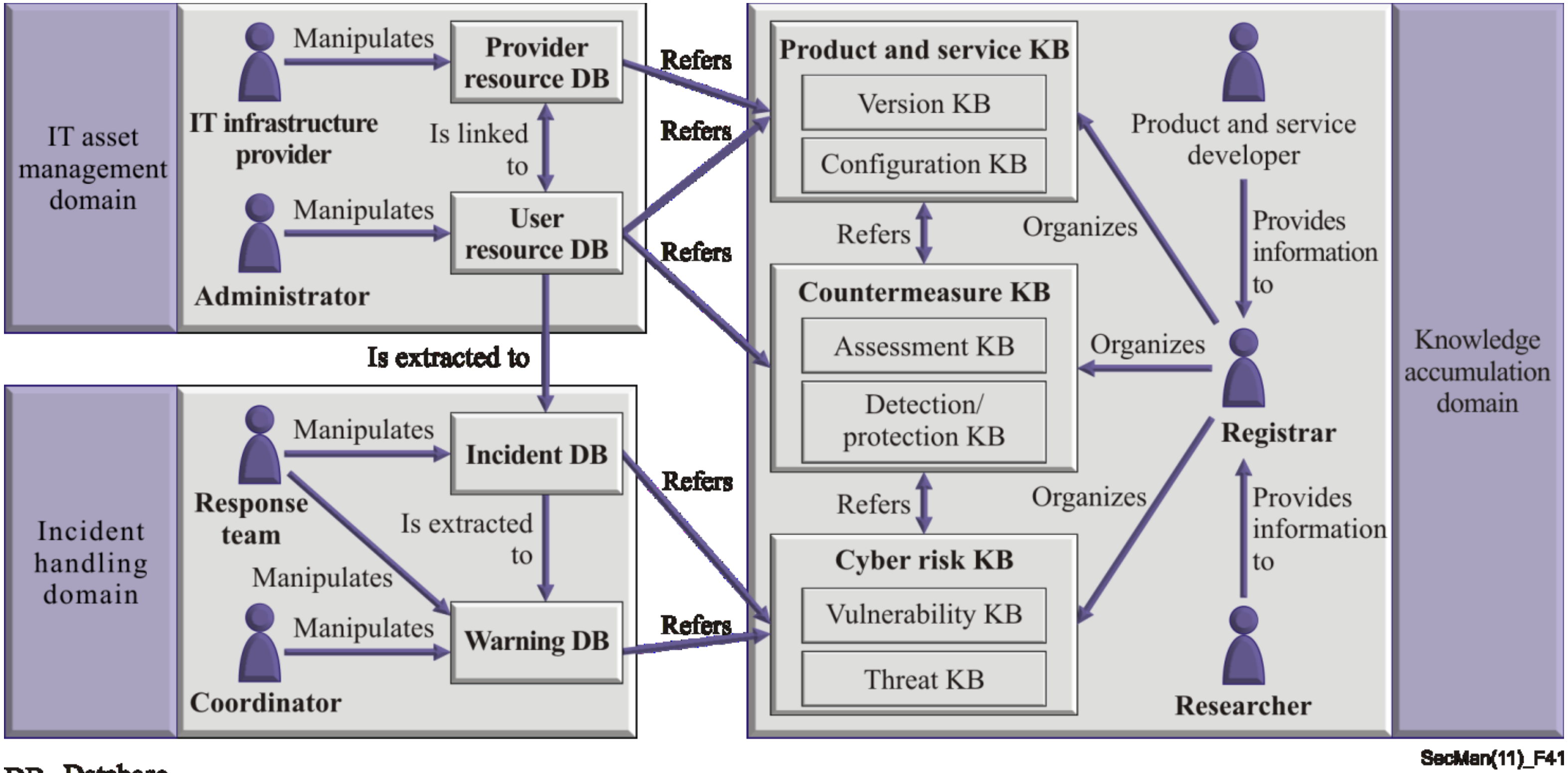
Product: $0.99_kindle_books

Version: 6

View CVEs

CYBEX identification and discovery

- Discovery mechanisms in the exchange of cybersecurity information (Rec. ITU-T X.1570)



DB	Database
KB	Knowledge base

Rec. ITU-T X.1570 - Cybersecurity operational information ontology

CYBEX event/incident/heuristics exchange

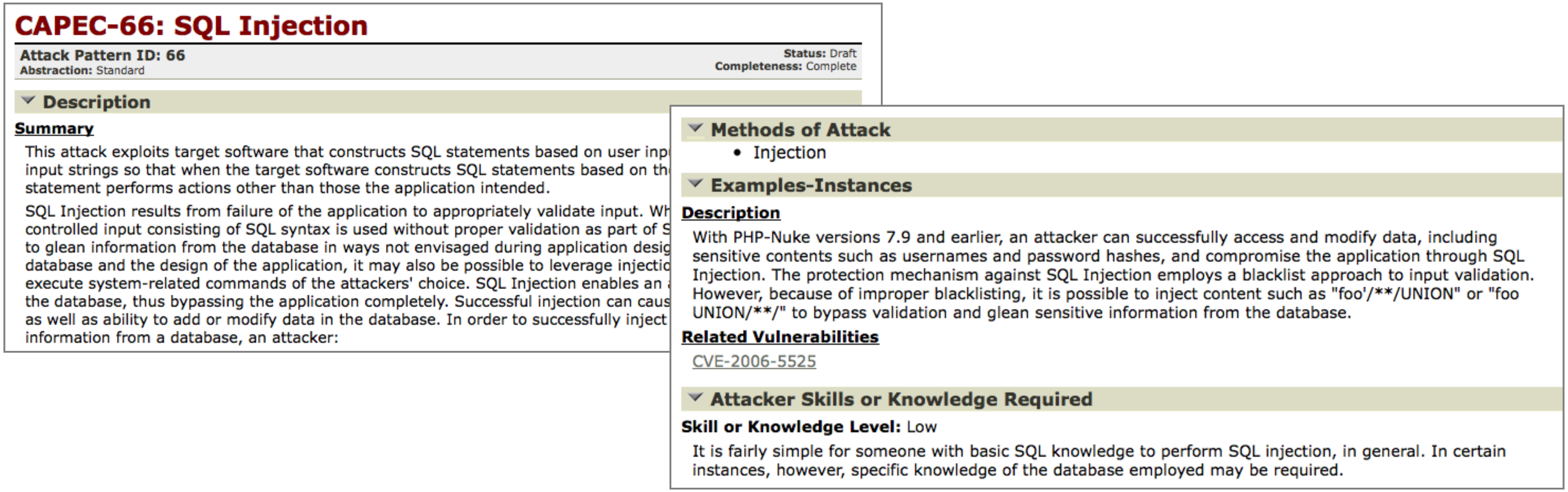
- Incident object description exchange format (IODEF) (Rec. ITU-T X.1541)
- describes the information model for IODEF format (IETF RFC 5070) and provides an associated data model specified with XML schema. IODEF specifies a data model representation for sharing commonly exchanged information about computer security or other incident types.
- IODEF enhances operational capabilities and improves situational awareness.

- The IODEF structured format (in XML Schema) allows for:
  - increased automation in the processing of incident information through the exchange of structured incident information, eliminating the need for security analysts to parse free-form textual documents;
  - decreased effort in correlating similar data (even when highly structured) from different sources enhancing situational awareness;
  - a common format on which to provide interoperability between tools for incident handling and analysis, specifically when information comes from multiple entities.

Knowledge base of attack patterns

- Common Attack Pattern Enumeration and Classification (CAPEC) (Rec. ITU-T X.1544)
  - Dictionary of attack patterns, solutions & mitigations
  - Facilitates communication of incidents, issues, as well as validation techniques and mitigation strategies
  - Community: http://capec.mitre.org/

CAPEC example: SQL injection



CAPEC-66: SQL Injection

Attack Pattern ID: 66
Abstraction: Standard

Status: Draft
Completeness: Complete

Description

Summary

This attack exploits target software that constructs SQL statements based on user inp
input strings so that when the target software constructs SQL statements based on th
statement performs actions other than those the application intended.

SQL Injection results from failure of the application to appropriately validate input. Wh
controlled input consisting of SQL syntax is used without proper validation as part of S
to glean information from the database in ways not envisaged during application desig
database and the design of the application, it may also be possible to leverage injectio
execute system-related commands of the attackers' choice. SQL Injection enables an a
the database, thus bypassing the application completely. Successful injection can caus
as well as ability to add or modify data in the database. In order to successfully inject
information from a database, an attacker:

Methods of Attack

- Injection

Examples-Instances

Description

With PHP-Nuke versions 7.9 and earlier, an attacker can successfully access and modify data, including sensitive contents such as usernames and password hashes, and compromise the application through SQL Injection. The protection mechanism against SQL Injection employs a blacklist approach to input validation. However, because of improper blacklisting, it is possible to inject content such as "foo'/**/UNION" or "foo UNION/**/" to bypass validation and glean sensitive information from the database.

Related Vulnerabilities

CVE-2006-5525

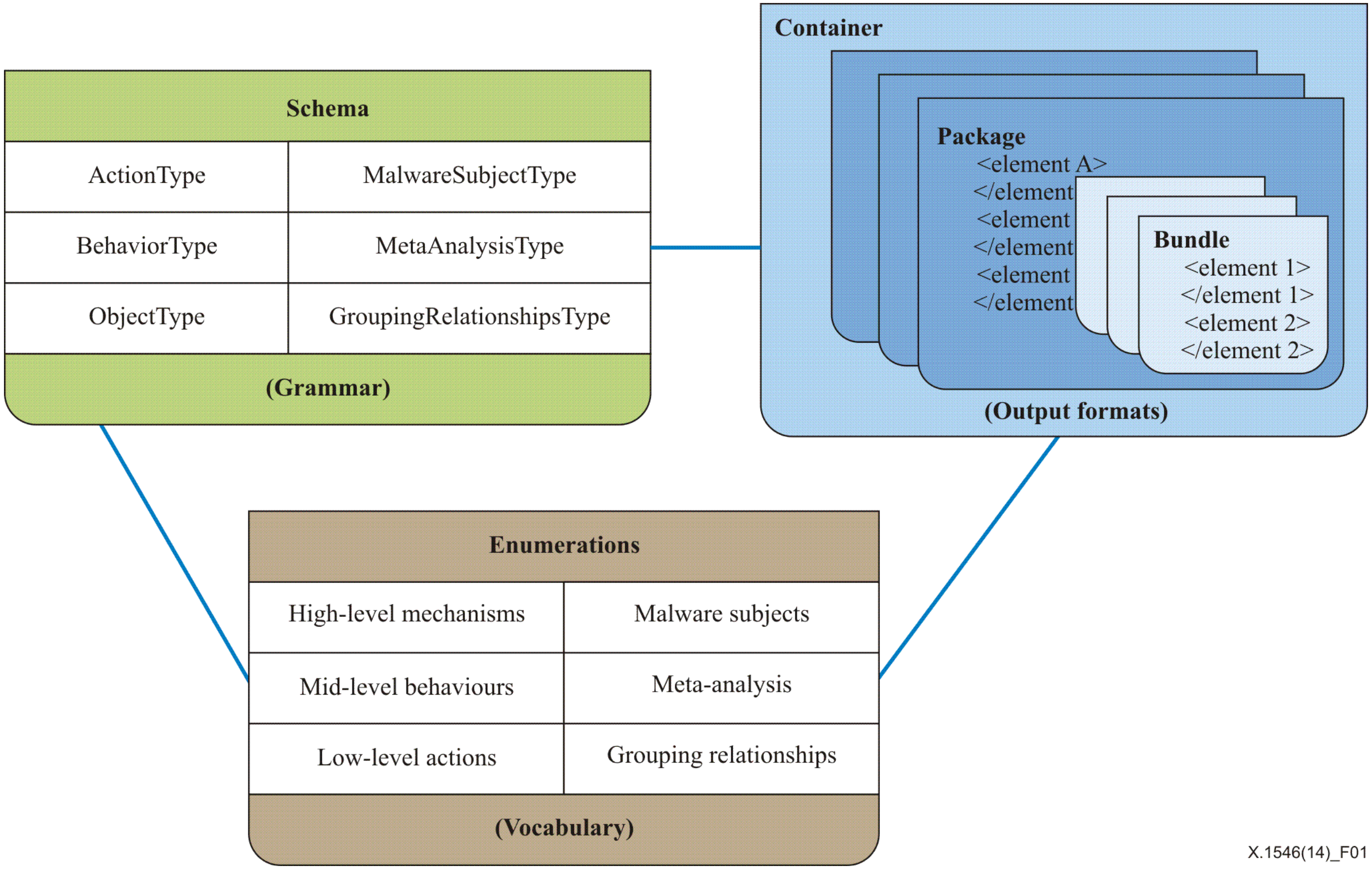
Attacker Skills or Knowledge Required

Skill or Knowledge Level: Low

It is fairly simple for someone with basic SQL knowledge to perform SQL injection, in general. In certain instances, however, specific knowledge of the database employed may be required.

CYBEX event/incident/heuristics exchange

- Malware attribute enumeration and classification (MAEC) (Rec. ITU-T X.1546)



Schema	
ActionType	MalwareSubjectType
BehaviorType	MetaAnalysisType
ObjectType	GroupingRelationshipsType
(Grammar)	

Enumerations	
High-level mechanisms	Malware subjects
Mid-level behaviours	Meta-analysis
Low-level actions	Grouping relationships
(Vocabulary)	

X.1546(14)_F01

Rec. ITU-T X.1546 – High-level MAEC overview

CYBEX assured exchange

- Real-time inter-network defence (RID) (Rec. ITU-T X.1580)
  - RID specifies a method to securely communicate incident information, enabling the exchange of IODEF XML documents.
  - conveys security, policy, and privacy controls to enable the exchange of potentially sensitive information.
  - RID includes provisions for secrecy, confidentiality, integrity and authentication for the exchange of incident information.
- Transport of real-time inter-network defence messages (Rec. ITU-T X.1581) (IETF RFC 6546)
  - specifies a transport protocol for RID messages over HTTP/TLS.
- Transport protocols supporting cybersecurity information exchange (Rec. ITU-T X.1582)

Summary

- ITU-T Study Group 17 developed international standards on security and on cybersecurity
  - The ITU-T X.1500-series of Recommendations on cybersecurity information exchange (CYBEX) provide critical instruments to deal with rapidly changing and diversifying cybersecurity phenomena, directly contributing to data protection
  - Enumeration standards provide effective means of communication across businesses, government agencies as well as communities
  - Cyber-risks are highly volatile and manifest through unexpected combination of components, that require careful examination of technical risks through knowledge-base standards.

Thank you very much for your attention!

Slides, abstracts, biographies of joint ITU/ATU Workshop on "Cybersecurity strategy in African countries“ freely available on ITU-T web-page at

http://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Pages/Programme.aspx

Backup

Question 4/17
Cybersecurity

- Recommendation in TAP approval process

For approval

  - **X.1542 (X.simef),** Session information message exchange format

- Recommendations on CYBEX currently under study include:

For agreement

  - **X.1500 Amd.10,** Overview of cybersecurity information exchange – Amendment 10 - Revised structured cybersecurity information exchange techniques

For determination

  - **X.nessa,** Access control models for incidents exchange networks

- Recommendations (non-CYBEX) currently under study include:

For determination

  - **X.cogent,** Design considerations for improved end-user perception of trustworthiness indicators
  - **X.metric,** Metrics for evaluating threat and resilience in cyberspace
  - **X.samtn**, Security assessment techniques in telecommunication/ICT networks
  - **X.sbb**, Security capability requirements for countering smartphone-based botnets

- In this study period, Q4/17 has developed eight new Recommendations (X.1208, X.1210, X.1211, X.1303*bis*, X.1525, X.1544, X.1546, X.1582), 3 revised Recommendations (X.1520, X.1521, X.1526), seven new Amendments (X.1500 Amds.3-9), 2 new supplements (X.Suppl.18, X.Suppl.20), and 1 revised supplement (X.Suppl.10).

CYBERSPACE SECURITY – Cybersecurity

- Overview of cybersecurity (Rec. ITU-T X.1205)
- A vendor-neutral framework for automatic notification of security related information and dissemination of updates (Rec. ITU-T X.1206)
- Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software (Rec. ITU-T X.1207)
- A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies (Rec. ITU-T X.1208)
- Capabilities and their context scenarios for cybersecurity information sharing and exchange (Rec. ITU-T X.1209)
- Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks (Rec. ITU-T X.1210)
- Techniques for preventing web-based attacks (Rec. ITU-T X.1211)

Reference links

- Webpage for ITU-T Study Group 17
  - http://itu.int/ITU-T/studygroups/com17
- Webpage on ICT security standard roadmap
  - http://itu.int/ITU-T/studygroups/com17/ict
- Webpage for JCA on child online protection
  - http://www.itu.int/en/ITU-T/jca/COP
- Webpage for JCA on identity management
  - http://www.itu.int/en/ITU-T/jca/idm
- Webpage on lead study group on security
  - http://itu.int/en/ITU-T/studygroups/com17/Pages/telesecurity.aspx
- Webpage on lead study group on identity management
  - http://itu.int/en/ITU-T/studygroups/com17/Pages/idm.aspx
- ITU Security Manual: Security in Telecommunications and Information Technology
  - http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf