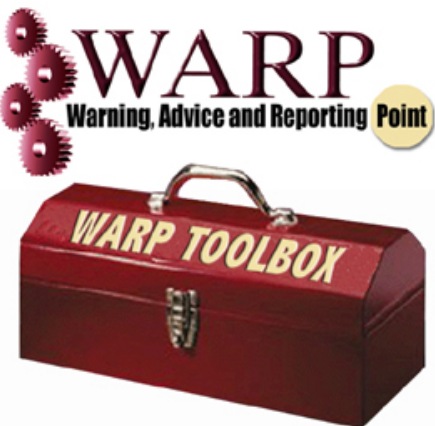


WARPs

(Warning, Advice and Reporting Points)

**WSIS Action Line C5 Facilitation Meeting:
“Partnerships for Global
Cybersecurity”**



John Harrison,
Consultant to
NISCC.

The common problem

- ICT networks and systems cannot be designed, built and operated which are 100% secure
- No one wants to admit supplying or operating vulnerable networks and systems – ICT does not carry a health warning!
- Detailed incident information is contained to minimise the risk to reputation
- Quantifying the problem (threat) is difficult because sharing information carries a risk
- ICT users and suppliers do not have the information to make informed decisions on the cost/benefit of improved security
- What should I do? When should I do it? What is the real threat? and what are others doing?

US Cybernotes 2003 – page 1



Department of Homeland Security Information Analysis and Infrastructure Protection Directorate CyberNotes

Issue #2003-26

December 31, 2003

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the Department of Homeland Security Information Analysis Infrastructure Protection Directorate Web site at <http://www.nipc.gov>.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a year-end summary of software vulnerabilities identified between December 6, 2002 and December 12, 2003. The table provides the vendor, operating system, software name, common name of the vulnerability, potential risk at the time of publication, and the CyberNotes issue in which the vulnerability appeared. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source indicated in the endnote.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text. Where applicable, the table lists a "CVE number" (in red)

NISCC

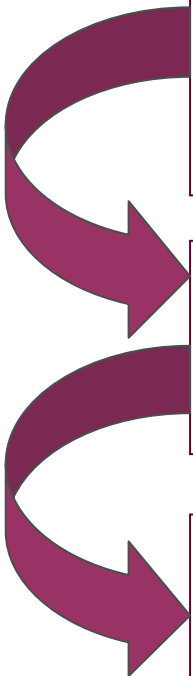
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

US Cybernotes 2003 – page 2

Vendor	Operating System	Software Name	Common Name	Risk*	CyberNotes Issue
3Com ⁷	Multiple	SuperStack 3 Firewall	SuperStack 3 Firewall Content Filter Bypassing	Medium	CyberNotes-2003-06
3Com ¹⁰	Multiple	SuperStack II RAS 1500	SuperStack II RAS 1500 Malicious IP Header Denial of Service & Inadequate Authentication	Low/Medium <i>(Medium if sensitive information can be obtained)</i>	CyberNotes-2003-07
3D-FTP ¹¹	Windows	3D-FTP Client 4.0	3D-FTP Client Buffer Overflow	High	CyberNotes-2003-09
3ware Software ¹²	Multiple	Disk Management Software 1.10.020, 1.10.012	Disk Management Denial of Service	Low	CyberNotes-2003-03
4D Inc. ¹³	Windows	WebSTAR 5.2-5.2.4, 5.3, 5.3.1	4D WebSTAR Remote Buffer Overflow	High	CyberNotes-2003-19
Abuse-SDL ¹⁴	Multiple	Abuse-SDL 0.7.0	Abuse-SDL Buffer Overflow	High	CyberNotes-2003-13
access_refuse. sourceforge.net ¹⁵	Unix	Apache mod_access_refuse 1.0.2	Apache Mod_Access_Refuse Remote Denial of Service	Low	CyberNotes-2003-08
access-remote- pc.com ¹⁶	Windows	Remote PC Access 2.1	Remote PC Access Denial of Service	Low	CyberNotes-2003-11
ACLogic ¹⁷	Multiple	CoaxFTP	CoaxFTP Remote Denial of Service		
Acme Laboratories ¹⁸ <i>See issues advisory¹⁹</i>	Unix	dtcpd 2.21b, 2.21, 2.22, 2.23b1	dtcpd default() Remote Buffer Overflow CVE Name: CAN-2003-089		
Acme Laboratories ²⁰ <i>Connectiva issues advisory²¹</i>	Unix	Acme mini_ttcpd 1.0 1, 1.0, 1.10-1.16, dtcpd 1.0, 1.90 a, 1.95, 2.0-2.23 b1	dtcpd/mini_ttcpd Director Traversal CVE Name: CAN-2002-1562		
ActivCard Corporation ²⁴	Windows XP	ActivCard Gold 1.21, 2.2	ActivCard Gold Cached Static Password	Medium	CyberNotes-2003-08
Active PHP Bookmarks ²⁵	Multiple	Active PHP Bookmarks 1.1.01	Active PHP Bookmarks Multiple File Include	High	CyberNotes-2003-01
Adalis Informations ²⁶	Unix	D-Forum 1.0, 1.10, 1.11	D-Forum Remote File Include	High	CyberNotes-2003-04
Adison GmbH ²⁷	Windows	Monitor Ware Agent 1.3, 5.4.21 SP1, 5.0 beta	WinSyslog Interactive Syslog Server Long Message Remote Denial of Service	Low	CyberNotes-2003-22
Adison GmbH ²⁸	Windows	WinSyslog 4.21 SP1	WinSyslog Long Syslog Message Remote Denial of Service	Low	CyberNotes-2003-21
Adobe Systems Inc. ²⁹	Windows	SVG Viewer 3.0 & prior	SVG Viewer Alert Method Code Execution	High	CyberNotes-2003-21
Adobe Systems Inc. ³⁰	Unix	Acrobat Reader (UNIX) 5.05-5.0.7, 4.05	Adobe Unix Acrobat Reader Buffer Overflow	High	CyberNotes-2003-14
Adobe Systems Inc. ³¹	Windows	SVG Viewer 3.0 & prior	SVG Viewer 'postURL' & 'getURL' Restriction Bypass	Medium	CyberNotes-2003-21
Adobe Systems Inc. ³²	Windows	SVG Viewer 3.0 & prior	SVG Viewer Active Scripting Security Bypass	Medium	CyberNotes-2003-21
Adobe Systems, Inc. ³³	Windows	Acrobat 5.0, 5.0.5	Acrobat JavaScript Parsing Engine	High	CyberNotes-2003-10
Adobe Systems, Inc. ³⁴ <i>Upgrade available & exploit virus³⁵</i>	Windows: 95/98/NT 4.0/2000, XP, MacOS, Unix	Acrobat 4.0 5, 4.0 5c, 4.0, 4.0 5 a, 5.0, 5.0.5, Acrobat Reader 4.0 5, 4.0 5c, 4.0, 4.0 5 a, 5.0, 5.0.5	Acrobat Plug-in Digital Signature CVE Name: CAN-2002-001	High	CyberNotes-2003-07 CyberNotes-2003-09
Aegis Group ³⁶	Windows	FoxWeb 2.5	FoxWeb Remote Buffer Overflow	High	CyberNotes-2003-19
ADIX ³⁷	Multiple	Mini-Webserver 1.1	Mini-Webserver Information Disclosure	Medium	CyberNotes-2003-14
akpop3d ³⁸	Unix	akpop3d 0.4-0.6, 0.7-0.7.5	akpop3d Authentication Code	Medium	CyberNotes-2003-18
Alabanza ³⁹	Multiple	AlaCart 1.0	AlaCart Authentication Bypass	High	CyberNotes-2003-25

Page 2 of 190

WARPs – A development model



Stage 1: Show the benefits of the WARP to the community through tailored **warning** service, so that everyone feels they are getting a personalised and valuable service.

Stage 2: Develop trust through encouraging members to help each other by sharing best practice and giving **advice** to each other through WARP facilities.

Stage 3: Encourage members to report their experiences of otherwise embarrassing attacks or problems (anonymously if necessary, through the operator) within the WARP collective learning.

WARP Member Benefits

- Better Protection of own systems
- Filtering service for Warnings & Advisories
 - saves resources
 - improves effectiveness
- Network for Advice, links, contacts
- Forum for Sharing of Best Practice
- Peer comparisons (rank, timing, resources)
- Highly Relevant Early Warnings
- Improved Awareness
- Reduced threat to everyone else

BS 7799 AND WARP

Information Security infrastructure

A.4.1

- Information security coordination specialist information security advice
- Cooperation between organisations

Responding to Security Incidents & Malfunctions

A.6.3

- Reporting security incidents
- Reporting security weaknesses
- Reporting software malfunctions
- Learning from incidents

Operational Procedures Responsibilities

A.8.1

Protection against Malicious Software

A.8.3

- Incident management procedures
- Controls against malicious software

User Training

A.6.2

- Information security education & training

WARPs

The WARP Register



The WARP TOOLBOX



WARP
Warning, Advice and Reporting Point



<http://www.warp.gov.uk>

Filtered Warnings Application

My Services

- My Subscription
- Alert Chronicle
- News Chronicle
- My Details

News

- News Management
- New News

Latest Five Alerts

- Low Severity Warning
Virus warning - W32/Bagz-D

- Low Severity Advisory
Bypassing MS Windows XP SP2 firewall

- Normal Severity Advisory
Multiple Vulnerabilities in Microsoft Internet Explorer

- Low Severity Advisory
Sun Solaris LDAP and RBAC Privilege Escalation Vulnerability

- Low Severity Advisory
RIM Blackberry Meeting Request Message "Location" Header DoS

Subscription Tree

Please select the categories of interest to you. To select a category or branch, simply tick the branch and all the items under it will be selected.

- This means there are one or more items in this category.
- This item has been selected but you have not yet saved your changes.

- All Categories
 - Good Practice
 - Incident/Threat
 - Target Groups
 - Incident Types
 - Motive & effect
 - Threat types
 - Vulnerabilities/Fixes
 - Cisco
 - HP
 - Linux/Apache

- Microsoft
 - MS Bundled Windows Software
 - MS Developer Products
 - MS Office/Business Products
 - MS Home Products
 - MS Server Products
 - MS Windows Operating Systems
 - Windows CE
 - Windows 2000
 - Windows XP
 - Windows 3.x
 - Windows 95
 - Windows 98
 - Windows NT
 - Windows 2003

- Sun Microsystems
- Apple

Save Close

- Microsoft
 - MS Bundled Windows Software
 - MS Developer Products
 - MS Office/Business Products
 - MS Home Products
 - MS Server Products
 - MS Windows Operating Systems
 - Windows CE
 - Windows 2000
 - Windows XP
 - Windows 3.x
 - Windows 95
 - Windows 98
 - Windows NT
 - Windows 2003

der a certain
mmit your

FWA Categories

My Services

- Search
- My Subscription
- My Account
- My Devices
- Logoff
- Technical Support

Notifications

- New WARP Alert V3
- New WARP News
- System Overview
- Trust Management
- Rule Management
- Device Management

Users

- User Management
- Signup Requests
- New User
- Groups

Tree Management

- Tree Management
- Configuration Management

Information

- Access Log
- Notification Log
- Statistics

Version 4.0 BETA 3
©Copyright 2004 NISCC, All Rights Reserved

Subscription Tree

Please select the categories of interest to you below, you can select as many or few as you like. If you want to receive Notifications for all items under a certain branch, simply tick the branch and all the sub-items will be selected automatically. When you are happy with your selection click 'Save' to commit your changes.

- This means there are one or more items selected below this branch.
- This item has been selected but you have not yet saved your changes

- All Categories
 - Good Practice
 - Incident/Threat
 - Vulnerabilities/Fixes
 - Cisco
 - HP
 - Linux/Apache
 - Microsoft
 - Sun Microsystems
 - Apple
 - Novell
 - IBM
- Local Government Applications
 - Parking systems
 - Langdale
 - Housing systems
 - Academy
 - Revs & Bens systems
 - Comino
 - SX3
 - Flex Systems
 - IBS
 - Electoral systems
 - MVM Pickwick
 - Stand
 - Finance systems
 - Selima
 - Cedar Systems
 - CRM systems
 - Lynx
 - McFarlane
 - Capita

- Local Government Applications
 - Parking systems
 - Langdale
 - Housing systems
 - Academy
 - Revs & Bens systems
 - Comino
 - SX3
 - Flex Systems
 - IBS
 - Electoral systems
 - MVM Pickwick
 - Stand
 - Finance systems
 - Selima
 - Cedar Systems
 - CRM systems
 - Lynx
 - McFarlane
 - Capita

Save Close



Setting up a WARP - the essentials

- The WARP Toolbox – www.warp.gov.uk
- A community (can be virtual)
- A ‘champion’
- The right ethos
 - NfP, cooperative, collaborative, enthusiastic
- Registration
- [Filtered Warning Software]

Developments

- FWA use by Uniras
- Common Advisory format
- Netherlands, Australia, USA
- ENISA
- Telcos
- MSP
- Police
- SMEs

The future

The WARPs Vision

- WARPs will become endemic across the UK, and beyond
 - Self-replicating
 - Free-standing
 - Co-operating
 - Improving the security of
 - their members
 - the CNI
 - Everyone else



A final thought

*“It is not from ourselves that we learn
to be better than we are”*

~Wendell Berry