

Document type: Reference

Typical information sources for a WARP Filtered Warnings Service

(V2.0) October 2006

Keywords

[Filtered Warnings Service, sources]

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk>

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

Contents

1	Scope	2
2	Definitions and abbreviations	2
2.1	Definitions	2
2.2	Abbreviations.....	2
3	Security information sources.....	2
3.1	CERTs.....	2
3.1.1	UK Government CERT (UNIRAS).....	2
3.1.2	US Government CERT (US-CERT).....	2
3.2	Vendor Sites.....	3
3.2.1	Microsoft	3
3.2.2	Symantec	3
3.2.3	Sophos	3
3.2.4	Cisco Systems.....	3
3.2.5	Sun Microsystems.....	3
3.2.6	Silicon Graphics	3
3.2.7	HP	4
3.2.8	ISS	4
3.2.9	RedHat Linux	4
3.2.10	Debian Linux	4
3.3	Service providers and third parties	4
3.3.1	Security Focus	4
3.3.2	MessageLabs	5
	History	5

1 Scope

This document provides links to some security information sources that can be used to feed the Filtered Warnings Service of a WARP. The list is not intended to be exhaustive in any way, it merely provides a useful starting point.

2 Definitions and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply:

CERT: Computer security incident response team, based on the model developed by the Carnegie Mellon University.

2.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

UNIRAS: Unified Incident Reporting and Alert Scheme

WARP: Warning, Advice and Reporting Point

3 Security information sources

3.1 CERTs

3.1.1 UK Government CERT (UNIRAS)

UNIRAS is the UK's government CERT and is a fully integrated part of NISCC. It responds to electronic attack and issues Warnings and Alerts regarding IT Security incidents and vulnerabilities.

URL – <http://www.uniras.gov.uk/>

3.1.2 US Government CERT (US-CERT)

US-CERT is a partnership between the US Department of Homeland Security and the public and private sectors. Established to protect the United States Internet infrastructure, US-CERT coordinates defence against and responses to cyber attacks across the US.

URL - <http://www.us-cert.gov/>

3.2 Vendor Sites

3.2.1 Microsoft

Microsoft security resource for IT professionals, home and business users alike along with Security Bulletins and patches for Microsoft products. Also provides some information on some current viruses.

URL – <http://www.microsoft.com/security/>

Mailing list - <http://www.microsoft.com/technet/security/bulletin/notify.msp>

3.2.2 Symantec

Symantec, a major security products vendor, provide excellent virus information along with very useful statistics.

URL – <http://securityresponse.symantec.com>

Mailing list - <http://nct.symantecstore.com/virusalert/>

3.2.3 Sophos

Sophos are an anti-virus software company. They provide a good source of information on the latest viruses along with news of current information security issues.

URL – <http://www.sophos.com/security/>

Mailing list - <http://www.sophos.com/security/notifications>

3.2.4 Cisco Systems

Cisco systems provide security alerts and patches for their own networking systems.

URL - <http://www.cisco.com/security/>

Mailing list - http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#subscribe

3.2.5 Sun Microsystems

Sun Microsystems provide security alerts and patches for their own computer systems and software.

URL - <http://sunsolve.sun.com/>

Mailing list - <http://sunsolve.sun.com/pub-cgi/show.pl?target=security/sec>

3.2.6 Silicon Graphics

Silicon Graphics provide security alerts and patches for their own computer systems and software.

URL – <http://www.sgi.com/support/security/>

Mailing list - <http://www.sgi.com/support/security/wiretap.html>

3.2.7 HP

HP provides security alerts and patches for all their operating system and software products.

URL - <http://www.software.hp.com/>

3.2.8 ISS

ISS produce security products, and maintain a computer security threat research team called Xforce. They therefore produce alerts and patches for their own products, and generate alerts on other vendor's products too.

URL - <http://xforce.iss.net/>

Mailing list- <https://atla-mm1.iss.net/mailman/listinfo/alert>

ISS also maintain an interesting “List of lists” - <http://xforce.iss.net/xforce/maillists/otherlists.php>

3.2.9 RedHat Linux

RedHat are a major Linux distributor, they provide advisories and patches for all the software elements distributed as RedHat Linux.

URL - <http://www.redhat.com/security/>

Mailing list - <http://www.redhat.com/mailman/listinfo/redhat-watch-list>

3.2.10 Debian Linux

Debian provides the major GNU distribution of Linux, and provides security alerts and patches for all the software elements contained within the distribution.

URL - <http://www.debian.org/security/>

Mailing list - <http://lists.debian.org/debian-security-announce/>

3.3 Service providers and third parties

3.3.1 Security Focus

Security Focus is a web site with a vast array of IT security information on all possible subjects. Security Focus operate the BUGTRAQ mailing list which is the original full disclosure mailing list for alerts and advisories (note this mailing list is high volume). Security Focus are owned by Symantec, but are operated as an independent organisation.

URL – <http://www.securityfocus.com>

Mailing lists – <http://www.securityfocus.com/archive>

3.3.2 MessageLabs

MessageLabs are a secure e-mail service provider, and are able to give real information regarding the current trends of e-mail borne attack based on the number of e-mails they block or clean for their clients.

URL – http://www.messagelabs.com/Threat_Watch

History

Version	Date	Description
V1.0	June 2004	First issue
V2.0	October 2006	Sources updated