



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 2, Issue 2

March 24, 2003

A BUSY WEEK ...

It has been a busy week on the vulnerabilities front. Microsoft, after a somewhat quiet time, has released three significant advisories in the past week.

- Flaw in Windows Script Engine could allow code execution.
- Flaw in ISA Server DNS Intrusion Detection Filter can cause denial of service.
- Unchecked buffer in

Windows component could cause web server compromise.

CERT/CC released an advisory relating to an 'integer overflow in the Sun RPC XDRlibrary routines', and MIT published a security advisory in relation to a cryptographic weakness in version 4 of the Kerberos protocol. wired.com published an article 'Leaked Bug Alerts Cause a Stir' which suggests that details of the Sun vulnerabil-

ity were released 'without authorisation'. This also applied to the release of information regarding the Kerberos bug and a third advisory about the OpenSSL security standard. The full article is available at Wired News.

Refer to the CCIP website: for links to recent vulnerability postings.

INSIDE THIS ISSUE:

Recent Significant Advisory & Alert list 2

More Net Attacks Loom, CERT says 2

CISSP (or SSCP) Exam Scheduled 3

Virus Activity 3

New Zealand Port Scan Activity 4

An Overview of Cross Site Scripting Attacks cont. 4

Mailing List 4

Reference List 4

Communication regarding this newsletter can be addressed to:

newsletter@ccip.govt.nz



Government
Communications
Security Bureau

CONTACT DETAILS

Ph: +64 4 498 7654
Fax: +64 4 498 7655

Email: info@ccip.govt.nz
Web: www.ccip.govt.nz

PO Box 12-209
Wellington, New Zealand

AN OVERVIEW of CROSS SITE SCRIPTING ATTACKS

Various websites and applications have been discovered to be vulnerable to Cross Site Scripting attacks (XSS - CSS refers to unrelated Cascading Style Sheets.) These vulnerabilities typically reveal users' private information. This can have extremely serious consequences both to the site and the user being targeted. It is important in designing or maintaining a website or application to understand what cross-site scripting attacks can do, and how to prevent them.

An XSS attack relies on a website displaying text without checking whether it contains special characters. The client browser interprets the special characters as script instructions, and executes the script. This script executes some malicious action, such as obtaining or modifying the user's cookies. The most commonly used Internet language is Hyper-Text

Markup Language (HTML), but any other language that the browser understands could also be used, e. g. Javascript, VB Script, ActiveX etc. The extra functionality of these languages could then be used maliciously by the attacker.

In a permanent cross-site scripting exploit, the website saves the information the attacker sends it. This input contains the XSS attack. An example of this is posting to a message board. Everyone viewing that message board will receive the attack code. A transient XSS attack is one that is constructed "on the fly" in response to a crafted Uniform Resource Locator (URL.) Some web pages, such as search engines, display portions of the URL web address in the page itself. If this URL contained scripting code, then that code would be displayed in the page. The attacker would send out a

crafted URL, and not need to change the hosting site in any way. The users would receive the attack code when they followed the link.

The attacker could put the attacking code on their own page, but this is likely to be less successful. The user is more likely to follow a link to a website that they already know. The URL can be obscured by expressing portions of it in hexadecimal notation. If the user often visits the site www.abc.com then "<http://www.abc.com/%20%20%22.html>" is less suspicious than other options may be, such as "<http://fly.to/evilhax0r.html>". The victim's computer may also have the exploited website listed in a group with fewer restrictions. This may allow the attacker to execute scripts and commands that would not otherwise be available. A website can only

(Continued on page 4)



RECENT SIGNIFICANT ALERT & ADVISORY LIST

REFERENCE	DESCRIPTION	DATE
MIT	Kerberos 5 - faulty length checks in xdrmem_getbytes	21/03/03
CERT/CC	Integer overflow in Sun RPC XDR library routines	20/03/03
Microsoft	Flaw In ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service	20/03/03
Microsoft	Flaw in Windows Script Engine Could Allow Code Execution	20/03/03
RedHat	New samba packages fix security vulnerabilities	19/03/03
OpenPKG	Security vulnerabilities in openssl, samba, mysql and apache	20/03/03
Debian	New tcpdump packages fix denial of service vulnerability	18/03/03
kde.org	KDE rlogin.protocol and telnet.protocol url kio vulnerability	18/03/03
Microsoft	Unchecked buffer in Windows component could cause web server compromise	18/03/03
MIT	Cryptographic weaknesses in Kerberos v4 protocol	18/03/03
RedHat	Updated linux 2.4 kernel fixes vulnerability	18/03/03
SuSE	buffer overflow in lprm	17/03/03
UNIRAS	Lotus: Notes/Domino Security vulnerabilities	17/03/03
@stake, Inc.	Sun ONE (iPlanet) Application Server Connector Module Overflow	14/03/03
HP	Potential vulnerability in hp jetdirect 310x	13/03/03

Please refer to the CCIP website for a more complete list of alerts and advisories.

The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed-denial-of-service- attack at any time.

More Net Attacks Loom, CERT says

MORE NET ATTACKS LOOM, CERT SAYS

The following is an extract from a recent eWeek article.

The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed-denial-of-service (DDoS) attack at any time, according to security officials.

Officials at the CERT Coordination Center said the organization is monitoring at least five large networks of compromised machines installed with so-called bots. The bots connect compromised PCs or servers to Internet Relay Chat Servers, which attackers commonly use to execute commands on the remote systems. At least one of these networks has more than 140,000 machines, officials said.

"We have seen indications that these networks are being used [for attacks]," said Marty Lindner, team leader

for incident handling at the CERT center at Carnegie Mellon University, in Pittsburgh. "The potential is there for them to cause serious long-term damage."

Unfortunately, CERT officials said, there is little they can do about a potential attack, other than sound the warning and hope users identify and patch infected machines.

CERT's dire warning is underscored by last week's emergence of the Deloder and Code Red.F worms. While neither worm does any immediate damage to infected machines, both install back doors that enable attackers to use compromised machines for future, much more damaging operations, such as DDoS attacks.

At the heart of this new trend, according to security experts, are poor security practices. But more impor-

tant is the mistaken belief by corporate IT that once crises such as those caused by Code Red or SQL Slammer die down, the trouble's over. In fact, after an initial flurry of advisories, warnings and patches, there are often months of years of sustained infections and residual DDoS attacks, Lindner said.

For example, Code Red reached its peak in July 2001 when more than 450,000 servers were infected and scanning for new targets. Since then, there are some 60,000 Code Red-infected machines scanning the Internet at any given time. Even a novice cracker would need only a tiny fraction of those machines to launch a devastating DDoS attack.

The full article is available at:
<http://www.eweek.com>

Port 445-MS-ds currently takes the lions share of probed ports worldwide.

New Zealand Port Scan Activity, page 4

CISSP (OR SSCP) EXAM SCHEDULED

The next CISSP (or SSCP) exam has been scheduled and is now on the (ISC)2 website for registration. The exam will be held on Saturday 16th of August 2003 at the Auckland KPMG office in Princess Street. To aid in preparation for the

CISSP exam, KPMG have also arranged to host the CISSP CBK Review Seminar. This will be held in Auckland from July 14th to 18th at a venue to be advised. The cost of the CBK Review Seminar is US\$2,495, with a discount of 10% if you register prior

to April 14th. The CBK Review Seminar should be listed on the (ISC)2 website by the end of this week for registrations.

For more details contact:
Paul Macpherson,
pmacpherson@kpmg.co.nz

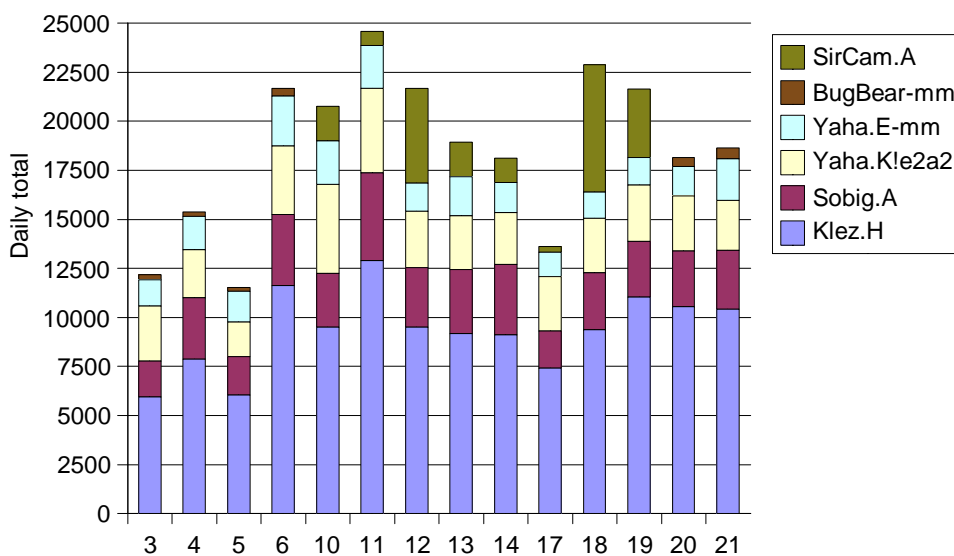
Cross Site Scripting attacks have been discovered in some well known and trusted sites, and have typically allowed users' private information to be accessed by attackers.

An Overview of Cross Site Scripting Attacks, page 1

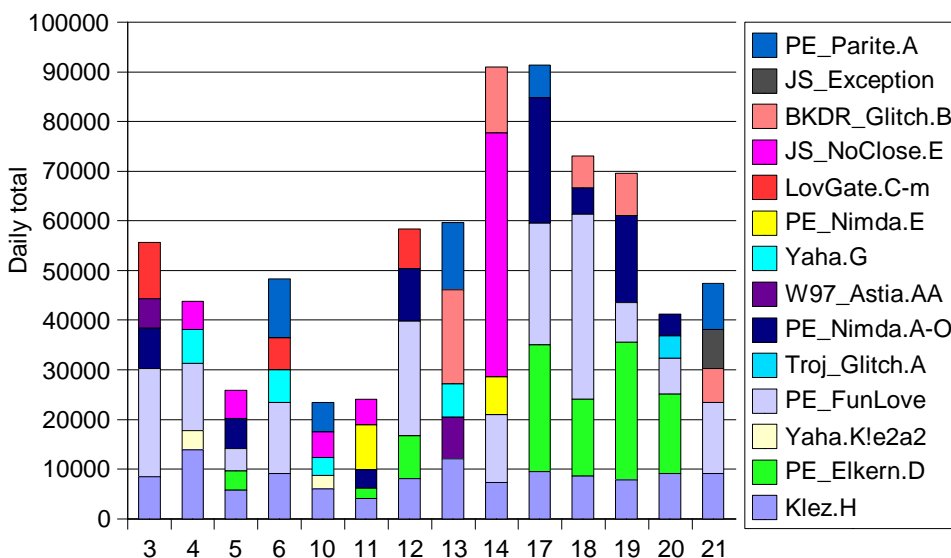
VIRUS ACTIVITY

Klez.h still features strongly in the MessageLabs data at about 50% for the last 20 days. TrendMicro has a different view of the world with PE_FunLove most prevalent 25% and Klez.h 15%.

Top 5 viruses captured worldwide by MessageLabs in March



Top 5 viruses captured worldwide by TrendMicro in March



Klez.h still features strongly in the MessageLabs data at about 50% for the last 20 days.

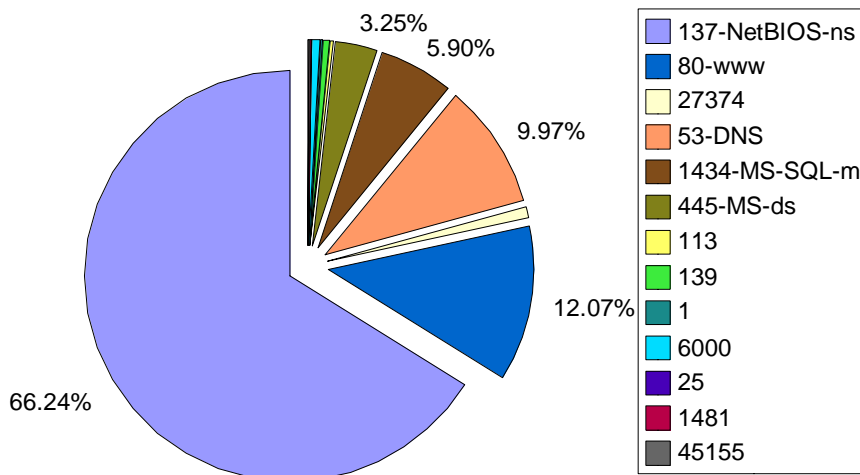
Virus Activity



NEW ZEALAND PORT SCAN ACTIVITY

This graph shows the port probe activity in NZ since the beginning of March. 137-NetBIOS-ns ranged between 5-10k probes per 24 hour period. Port 445-MS-ds currently takes the lions share of probed ports worldwide.

New Zealand's port probe activity by port number during March from incidents.org



OVERVIEW of CROSS SITE SCRIPTING ATTACKS CONT.

(Continued from page 1)

obtain information in cookies previously sent out by that website. By hosting the attack code on the victim website, the attacker can gain access to cookies from that website. This information would not be available from the attacker's own website.

Any situation in which a user can enter data that will be displayed on-line may be

vulnerable to an XSS attack. However, the attacks rely on the client browser interpreting the text as machine instructions. Some characters define computer instructions, such as "<" and ">" in the case of HTML, or "(" and ")" for javascript. Any user input should be checked for these characters, and (if found) replaced with their pedantic (but safe) equivalents, such as < (which is displayed as "<"). In this

manner the client browser will recognise that the text is only text, and not any scripting language. All input should be validated, and only known characters accepted, with other characters either being replaced, or removed altogether.

For further information, see: "HTML Code Injection and Cross-site scripting" at <http://www.technicalinfo.net/papers/CSS.html>

MAILING LIST

Critical alerts will be emailed to members of the CCIP email list as and when we become aware of them.

To subscribe, send your con-

tact details by email with the subject line: 'Subscribe' to alerts@ccip.govt.nz. To unsubscribe, send an email with the subject line: 'Unsubscribe' to the same

address.

This service is intended for CI organisations, government departments and IT service providers in New Zealand.

REFERENCES

eWeek: www.eweek.com
 MessageLabs: www.messagelabs.com
 Internet Storm Centre: isc.incidents.org

ISC2: www.isc2.org
 TrendMicro: www.trendmicro.com
 Technical Info: www.technicalinfo.net

DISCLAIMER

While this newsletter is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this newsletter.

CCIP only issues those external alerts that we assess as serious and would affect a large number of NZ users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this newsletter in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions stressed herein may not be used for advertising or product endorsement purposes.

Please refer to the CCIP website for a list of recent alerts and advisories.



CONTACT DETAILS

Ph: +64 4 498 7654
 Fax: +64 4 498 7655

Email: info@ccip.govt.nz
 Web: www.ccip.govt.nz

PO Box 12-209
 Wellington, New Zealand