Critical Vulnerability Analysis

The Weekly Email Update On Vulnerabilities Requiring Action

- Sign up now at https://server2.sans.org/sansnews

Keeping up with new vulnerabilities is easier with SANS free Critical Vulnerability Analysis (CVA) email update. The CVA, arriving in email boxes every Monday morning, saves time for security managers and system administrators by **providing authoritative answers** to three questions:

Answers three essential questions

1. **Which of the 30 to 50 vulnerabilities discovered in the preceding week are important enough that they demand action?**
2. **What is known about how the vulnerability works, what software it impacts, how bad the damage could be, how easily the vulnerability can be exploited, and how to correct the problem?**
3. **How have expert security practitioners in large organizations gone about prioritizing and correcting the problem?**

How Does It Work?

Starting with the last question, here's how the process works.

The "Security Council"

A Council of fifteen security experts, representing some of the largest computer user organizations in North America (banks, research centers, universities, government agencies, ISPs, and more) review the high priority vulnerabilities and report what they have done to correct the problem or to protect their systems through perimeter controls. Since the members of the Council are responsible for overseeing security action for their organizations, their actions are very practical. Obviously their identities and their employers' identities are secret. Their actions are summarized in the "Council Site Actions" section.

To determine which of the dozens of new vulnerabilities demand action, the Council established a prioritization process that takes into account how widely the vulnerable software is deployed, how much damage an exploit can do,

Sign up now at https://server2.sans.org/sansnews

Sign up now at https://server2.sans.org/sansnews

and whether an exploit is already available or how easy it would be to create one. Vicki Irwin, a senior security engineer at Tipping Point, and one of the nation's most respected security gurus, takes on the weekly job of applying the criticality criteria to each of the 30 to 50 vulnerabilities listed in the Security Alert Consensus (subscribe free at http://server2.sans.org/sansnews), the definitive weekly summary of newly discovered vulnerabilities.

Vicki also adds to the information provided in the Security Alert Consensus, providing additional details on how the vulnerability works and how to correct the problem.

Who Gets the CVA?

The distribution system for the CVA is a cascade in which the chief information security officer, the operations head, the CIO and/or the audit director register their organization and register redistribution lists containing persons inside their organizations who are in a position to find and correct the critical vulnerabilities. In this way, hundreds of thousands of technical security and systems and network administrators can get the report efficiently and quickly.

A First Alert Network For Rapid Action

The cascade will also be used as a First Alert Network to make sure the broadest possible group of people can be informed quickly when a virulent new worm or other widespread attack has been launched on the Internet.

- Sign up now at https://server2.sans.org/sansnews

Three pages of one issue and the table of contents of two other issues are shown on the following pages:

- Sign up now at https://server2.sans.org/sansnews

****

SANS Critical Vulnerability Analysis

September 30, 2002 Vol. 1. No. 10

****

Summary: Every Monday, the CVA prioritizes and summarizes the most important vulnerabilities identified during the past week and provides data on actions taken by security and systems managers at fifteen very large organizations (the Council) to protect their computers and networks from exploits of the reported vulnerabilities.

See "About the CVA Process and Council" at the end of this note for more data on how the report is compiled.

****

TABLE OF CONTENTS:

****

DETAILED SUMMARIES OF THE VULNERABILITIES AND COUNCIL ACTIONS:

(1) HIGH: Microsoft Windows: JVM Code Execution Vulnerability

Affected Products:
Potentially all versions of Windows.
Windows 95/98/98SE/ME/NT/2000/XP are known to be affected.
Any Windows machine running the Microsoft Java Virtual Machine (VM) up to and including build 5.0.3805 is affected.

Description:
The Microsoft Java Virtual Machine (VM), shipped with virtually all versions of Windows and Internet Explorer, has been found to contain three vulnerabilities. The most critical issue is that a malicious Java applet can execute arbitrary code on a victim Windows system. A hostile applet could be delivered by a malicious website or email message, and can execute arbitrary code with the privileges of the user running the applet.

Risk: Client compromise.
A hostile Java Applet can take any action on a victim Windows system, with the privileges of the user running the applet.

Deployment: Huge.
The vulnerability affects virtually all versions of Windows and Internet Explorer.

Ease of Exploitation: Appears to be straightforward.
Any applet may access the functions provided by JVM's XML support

class. The bug arises because some of these functions should only be available to trusted Java programs. One of the accessible functions allows applets to manipulate the contents of system memory.

Status: Vendor confirmed, patch available.

Reference:
Microsoft Security Bulletin MS02-052:
http://www.microsoft.com/technet/security/bulletin/MS02-052.asp

Council Site Actions:
Most of the reporting council sites are running the affected software. Those sites all notified their desktop support groups of the vulnerability and are planning to deploy the patches during the next regularly scheduled patch update. Several of the council sites stated their firewall ACL rules (blocks JAVA) and Anti-virus strategy protects their internal hosts from potential compromise through these vulnerabilities. Thus, deployment of patches can wait for the regular patch schedule.

---more –

****

EXPLOIT CODE RELEASES:

(1) vBulletin Calendar.php: Remote Command Execution Exploit

Affected Products:
vBulletin versions 2.2.0 and prior

Description:
This exploit allows remote attackers to execute arbitrary shell commands on web servers running vBulletin's calendar.php software, with the privileges of the server process. The exploit appears to have an (intentional?) bug that sends a stack dump from the attacker's machine in the attack packet (a malicious HTTP GET request). The stack dump reveals sensitive information about the attacker's machine and environment. According to the SecuriTeam advisory, the vulnerability has been fixed in version 2.2.8 of vBulletin. We were unable to get immediate confirmation of the problem, fix or any other information from the vendor.

Exploit Code:
http://www.securiteam.com/exploits/5QP0P158AC.html
http://packetstormsecurity.nl/0209-exploits/vbull.c

Council Site Actions:
The affected software is not in production or widespread use at any of the council sites. They reported that no action was necessary.

****

(2) Additional Exploits for OpenSSL SSLv2 Handshake Vulnerability

Affected Products:
Systems running OpenSSL v. 0.9.6d and earlier

Description:
Additional code has been posted that exploits the OpenSSL SSLv2

handshake vulnerability. This vulnerability was recently exploited by
the "Slapper" worm (discussed in last week's newsletter). Standalone
code that exploits the vulnerability has been published, and two new
worm variants have been discovered in the wild.

Standalone exploits, code apparently taken from the Slapper worm:
http://packetstormsecurity.nl/0209-exploits/apache-ssl-bug.c
http://packetstormsecurity.nl/0209-exploits/apache-linux.txt

Standalone exploit, possibly original code:
http://packetstormsecurity.nl/filedesc/openssl-too-open.tar.html

New worm variants: Cinik and Unlock
http://securityresponse.symantec.com/avcenter/venc/data/linux.slapper.worm.html
http://isc.incidents.org/analysis.html?id=169

Council Site Actions:
The release of additional exploit code did not alter the actions of
the council sites. For those sites affected by the vulnerable code,
they had already responded to the previous announcements.

One of the council sites reported that they were able to construct
their own standalone exploit code within an hour of first obtaining
the worm source code, and they have operated under the expectation
that this task would be similarly easy for a large number
of potential intruders. They also reported that in addition to the
dozen systems at their site that were compromised only by the worm,
they found one system that was compromised both by the worm and by a
separate exploitation of the same vulnerability. (It had a large
collection of uploaded files, such as IRC proxy-server software, that
were owned by the username under which the Apache web server ran.)

****

-- snip --

****
SANS Critical Vulnerability Analysis
September 23, 2002 Vol. 1. No. 9
****

TABLE OF CONTENTS:
Widely Distributed Software:
 (1) CRITICAL: Linux Apache OpenSSL Peer-to-Peer Worm (Various Names)
Other Software:
 (2) MODERATE: PlanetWeb Web Server Long URL Buffer Overflow
 (3) MODERATE: Heimdal Kerberos (NetBSD) kfd Daemon Buffer Overflow
 (4) LOW: Savant Web Server cgitest.exe Buffer Overflow
****

-- snip --

- Sign up now at https://server2.sans.org/sansnews

****
SANS Critical Vulnerability Analysis
September 16, 2002 Vol. 1. No. 8
****

****

TABLE OF CONTENTS:

****

==end==

- Sign up now at https://server2.sans.org/sansnews