CERT Advisory CA-2001-11 sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: May 10, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred to here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934
http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems. For additional information about this vulnerability, see

http://www.kb.cert.org/vuls/id/111677

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

- Sample syslog entry from compromised Solaris system

```
May  7 02:40:01 carrier.example.com inetd[139]: /usr/sbin/sadmind: Bus Error - core dumped
May  7 02:40:01 carrier.example.com last message repeated 1 time
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault - core dumped
May  7 02:40:08 carrier.example.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.example.com last message repeated 1 time
May  7 02:44:14 carrier.example.com inetd[139]: /usr/sbin/sadmind: Killed
```

- A rootshell listening on TCP port 600
- Existence of the directories
  - /dev/cub *contains logs of compromised machines*
  - /dev/cuc *contains tools that the worm uses to operate and propagate*
- Running processes of the scripts associated with the worm, such as the following:
  - /bin/sh /dev/cuc/sadmin.sh
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
  - /dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
  - /bin/sh /dev/cuc/uniattack.sh
  - /bin/sh /dev/cuc/time.sh
  - /usr/sbin/inetd -s /tmp/.f
  - /bin/sleep 300

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

- Modified web pages that read as follows:

```
fuck USA Government
   fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn
```

- Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/system32/cmd.exe /c+dir+..\ 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
          GET /scripts/root.exe /c+echo+&LT;HTML code inserted here>.././index.asp 502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:

http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull /191&type=0&nav=sec.sba

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)* http://www.kb.cert.org/vuls/id /111677
2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind*
   http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, John Shaffer

Revision History

May 08, 2001: Initial Release
May 08, 2001: Formatting change to improve printing
May 08, 2001: Correct link in the vendor section to point to the correct Microsoft Bulletin.
Our apologies to Microsoft for the error.
May 10, 2001: Changed sanitized logs to example.com