CERT Advisory CA-1992-15 Multiple SunOS Vulnerabilities Patched

Original issue date: July 21, 1992
Last revised: September 19, 1997
Attached copyright statement

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

*** This advisory supersedes CA-91.16. ***

The CERT/CC (Computer Emergency Response Team/Coordination Center) has received information concerning several vulnerabilities in the Sun Microsystems, Inc. (Sun) operating system (SunOS). These vulnerabilities affect all architectures and supported versions of SunOS including 4.1, 4.1.1, and 4.1.2 on sun3, sun3x, sun4, sun4c, and sun4m. The patches have been released as upgrades to three existing patch files.

Since application of these patches involves rebuilding your system kernel file (/vmunix), it is recommended that you apply all patches simultaneously. Use the procedure described below to apply the patches and rebuild the kernel.

Sun has provided patches for these vulnerabilities as updates to Patch IDs 100173, 100376, and 100567. They are available through your local Sun Answer Centers worldwide as well as through anonymous ftp from the ftp.uu.net (137.39.1.9) system (in the /systems/sun/sun-dist directory).

```
Fix                    Patch ID      Filename           Checksum
NFS Jumbo              100173-08     100173-08.tar.Z     32716    562
Integer mul/div        100376-04     100376-04.tar.Z     12884    100
ICMP redirects         100567-02     100567-02.tar.Z     23118     13
```

Please note that Sun Microsystems sometimes updates patch files. If you find that the checksum is different please contact Sun Microsystems or CERT for verification.

NFS jumbo patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, all architectures

I. Description
The upgrade to the NFS Jumbo patch addresses a vulnerability that allows an intruder to become root using NFS. This vulnerability affects all architectures and supported versions of SunOS.

II. Impact
A remote user may exploit this vulnerability to gain root access.

III. Solution
Extract the new files to be installed in the kernel.

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

Integer mul/div patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, SPARC architectures

I. Description
The integer mul/div patch upgrade addresses an additional problem with the integer multiplication emulation code on SPARC architectures that allows an intruder to become root. This vulnerability affects SPARC architectures (sun4, sun4c, and sun4m) for all supported versions of SunOS (4.1, 4.1.1, and 4.1.2).

II. Impact
A local user may exploit a bug in the emulation routines to gain root access or crash the system.

III. Solution
Extract the new files to be installed in the kernel. Note that this patch applies only to SPARC architectures.

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

ICMP redirects patch upgrade, SunOS 4.1, 4.1.1, 4.1.2, all architectures

I. Description
The ICMP redirects patch addresses a denial of service vulnerability with SunOS that allows an intruder to close existing network connections to and from a Sun system. This vulnerability affects all Sun architectures and supported versions of SunOS.

II. Impact
A remote user may deny network services on a Sun system.

III. Solution
Extract the new file to be installed in the kernel (the patch is the same for all supported versions of SunOS).

Install the patch files in /sys/`arch -k`/OBJ as described in the README file included in the patch file. Be sure to make a backup of each of the files you are replacing before moving the patched file to the /sys/`arch -k`/OBJ directory.

Config, make, and install the new kernel to include all patches described in this advisory appropriate to your system. Reboot each host using the appropriate kernel. Refer to the Systems and Network Administration manual for instructions on building and configuring a new custom kernel.

The CERT/CC wishes to thank Helen Rose of the EFF, Gordon Irlam of the University of Adelaide, Wietse Venema of Eindhoven University, and Ken Pon at Sun Microsystems, Inc for their assistance.

Revision History

```
September 19,1997   Attached copyright statement
```