CERT Advisory CA-2001-34 Buffer Overflow in System V Derived Login

Original release date: December 12, 2001
Last revised: April 11, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Cisco applications running on a unpatched Sun Solaris OS
- Hewlett-Packard's HP-UX
- IBM AIX versions 4.3 and earlier and 5.1
- SCO OpenServer 5.0.6a and earlier
- SGI IRIX 3.x
- Sun Solaris 8 and earlier

Overview

Several applications use *login* for authentication to the system. A remotely exploitable buffer overflow exists in *login* derived from System V. Attackers can exploit this vulnerability to gain root access to the server.

I. Description

Several implementations of *login* that are derived from System V allow a user to specify arguments such as environment variables to the process. An array of buffers is used to store these arguments. A flaw exists in the checking of the number of arguments accepted. This flaw permits the array of buffers to be overflowed.

On most systems, *login* is not suid; therefore, it runs as the user who called it. If, however, *login* is called by an application that runs with greater privileges than those of the user, such as telnetd or rlogind, then the user can exploit this vulnerability to gain the privileges of that program. In the case of telnetd or rlogind, root access is gained.

Since in.telnetd and in.rlogind are available over the network, a remote attacker without any previous access to the system could use this vulnerability to gain root access to the system.

If a program that invokes *login* is suid (or sgid) USER_A, then this can be exploited to gain the privileges of USER_A.

An exploit exists and may be circulating.

II. Impact

This vulnerability can be remotely exploited to gain privileges of the invoker of *login*. In the case of a program such as telnetd, rlogind, or other suid root programs, root access is gained.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please review VU#569272 for your vendor's status or contact your vendor directly.

Restrict access to login

We recommend disabling TELNET, RLOGIN and other programs that use *login* for authentication. Do not use programs that use a vulnerable *login* for authentication. Note that some SSH applications can be configured to use *login* for authentication. If this configuration is selected, then you will still be vulnerable.

If you cannot disable the service, you can limit your exposure to these vulnerabilities by using a router or firewall to restrict access to port 23/TCP (telnet) and port 513/TCP (rlogin). Note that this does not protect you against attackers from within your network.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server are not vulnerable.

Caldera

We are not using a SystemV based /bin/login, we are using the BSD originated rlogin tools. All OpenLinux products are 'Not Vulnerable'.

Cisco

See http://www.cisco.com/warp/public/707/Solaris-bin-login.shtml

Compaq Computer Corporation
Compaq's Tru64 Software is not impacted by this reported problem.
Cray Inc.
Cray Inc. has determined that its implementation of login is not vulnerable to the situation described in VU#569272.
Hewlett-Packard

HP-UX is NOT Exploitable. It is NOT a security issue with HP-UX. HP-UX does have a benign buffer overflow which is the only reason HP-UX is listed as "effected" above. In any case, the buffer overflow has been fixed by HP.
IBM

IBM's AIX operating system, versions 4.3 and 5.1, are susceptible to this vulnerability. We have prepared an emergency fix ("efix"), "tsmlogin_efix.tar.Z", and it is available for downloading from:
ftp://aix.software.ibm.com/aix/efixes/security

The APAR assignment for AIX 5.1 is IY26221. The APAR for AIX 4.3 is IY26443. Both will be available soon. The "README" file at the above FTP site will be updated to provide the official fix information and availability.

Update: Incomplete installation instructions were included in the first posting of the efix on Wednesday, 12 December 2001. The installation instructions were rewritten and tarballed with the efixes. The efix tarball was then reposted to the FTP download site on the afternoon of Thursday, 13 December. An amended advisory reflecting the correct instructions has also been issued. Customers may wish to consult the amended advisory, or download the most recent efix, to obtain the new instructions.

IBM is developing an emergency fix for AIX 4.2.1 at Maintenance Level 06 (the last ML done). Also, we are developing efixes for AIX 4.3.3 at maintenance levels 06 and 08.
NetBSD
NetBSD does not use a System V derived login, and therefore, NetBSD is not vulnerable.
Red Hat
Red Hat Linux does not use a System V derived /bin/login, and is therefore not vulnerable to this.
SCO

Open UNIX 8 and UnixWare are not vulnerable to this login issue.

ftp://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.40/CSSA-2001-SCO.40.txt
SGI

SGI Has released a security bulletin to address this issue.
Sun Microsystems

Sun has developed a fix and T-patches are being tested. Official patches will be released shortly and Sun will issue a Sun Security Bulletin when they are available.

Update: Sun has released a security bulletin and patches for this issue.

The CERT Coordination Center thanks Internet Security Systems and Sun Microsystems for the technical information they provided.

Feedback on this document can be directed to the author, Jason A. Rafail

---

References

- http://www.kb.cert.org/vuls/id/569272
- http://www.kb.cert.org/vuls

Revision History

```
December 12, 2001: Initial Release
December 13, 2001: Update Hewlett-Packard Vendor Statement
December 14, 2001: Added SCO Vendor Statement
December 14, 2001: Updated IBM Vendor Statement
December 14, 2001: Updated Systems Affected
December 17, 2001: Updated Sun Microsystems Vendor Statement
December 18, 2001: Updated IBM Vendor Statement
December 18, 2001: Added SGI Vendor Statement
April 11, 2002: Added Cisco Vendor Statement
```