

[UNIX] Solaris fs.auto Remote Compromise Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0090.html>

From: support@securiteam.com

Date: 11/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: 26 Nov 2002 11:52:44 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Solaris fs.auto Remote Compromise Vulnerability

SUMMARY

ISS X-Force has discovered a vulnerability in the Sun Microsystems implementation of the "X Window Font Service", or "XFS". The XFS service was designed as a component of the X Windows systems to establish a common mechanism to export font data to all computers on an X Windows network. A buffer overflow vulnerability exists within the XFS service (fs.auto).

DETAILS

Affected Versions:

- * Sun Microsystems Solaris 2.5.1 (Sparc/Intel)
- * Sun Microsystems Solaris 2.6 (Sparc/Intel)
- * Sun Microsystems Solaris 7 (Sparc/Intel)
- * Sun Microsystems Solaris 8 (Sparc/Intel)
- * Sun Microsystems Solaris 9 (Sparc)
- * Sun Microsystems Solaris 9 Update 2 (Intel)

The XFS protocol is used by computers on an X Windows network to share font information. The X Windows system implemented an extensive and scalable font capability. This capability requires that all X Windows clients and servers have a mechanism to access font data, which may be

Securiteam: [UNIX] Solaris fs.auto Remote Compromise Vulnerability

distributed throughout an X Windows network.

Solaris implemented the XFS font server in the daemon, fs.auto. A flaw exists within the fs.auto Dispatch() routine. Adequate bounds-checking is not conducted on user-supplied data within the vulnerable function. This flaw can allow remote attackers to formulate a specific XFS query to either crash the service, or execute arbitrary code under the privilege of the "nobody" user. This privilege level is similar to that of any normal user.

Impact:

Remote attackers can exploit the buffer overflow vulnerability to run arbitrary commands on a target system. Attackers must exploit this vulnerability in conjunction with another attack to gain "root" access, because the fs.auto service does not run with superuser privilege. The Solaris operating system is configured to run the fs.auto service by default. It is bound to a high TCP port, which is normally blocked on perimeter firewalls. Networks that are not filtering high TCP ports, and internal networks are potentially at risk.

Recommendations:

X-Force recommends that administrators disable the fs.auto service unless it is explicitly required. Administrators can disable fs.auto by editing the inetd configuration file (/etc/inetd.conf) and then restart the inetd process by following the steps below:

1. Comment out the line corresponding to fs.auto. It should read:

```
#fs stream tcp wait nobody /usr/openwin/lib/fs.auto  
fs
```

2. Restart the inetd process

```
# ps -ef |grep inetd  
root 138 1 0 Oct 15 ? 0:00 /usr/sbin/inetd -s  
# kill -HUP 138
```

Administrators should inspect their network perimeters to insure that strong packet filtering rules are in place. The XFS protocol uses TCP port 7100. This port should be blocked on all network perimeters.

Vendor Notification Schedule:

Vendor confirmed patches would be available on 11/25/2002, and has since rescheduled the patch release after the publication of this advisory. Please contact Sun for more information.

Initial vendor notification: 10/16/2002

Initial vendor confirmation: 10/17/2002

Final release schedule agreement: 11/18/2002

ADDITIONAL INFORMATION

Securiteam: [UNIX] Solaris fs.auto Remote Compromise Vulnerability

The original advisory can be downloaded by going to:

<<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>>
<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>

The information has been provided by <mailto:xforce@iss.net> X-Force.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.