

[UNIX] Multi-Vendor Format String Vulnerability in ToolTalk Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0007.html>

From: support@securiteam.com

Date: 10/03/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] Multi-Vendor Format String Vulnerability in ToolTalk Service

Message-Id: <20011003212037.3B234138C4@mail.der-keiler.de>

Date: Wed, 3 Oct 2001 23:20:37 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Multi-Vendor Format String Vulnerability in ToolTalk Service

SUMMARY

ISS X-Force has discovered a format string vulnerability in the ToolTalk RPC service present on many commercial UNIX variants. The ToolTalk database server (rpc.ttdbserverd) contains a format string vulnerability that may allow remote attackers to crash the ToolTalk service, or execute arbitrary code on a target system with super user privilege.

DETAILS

Vulnerable systems:

HP HP-UX 10.10

HP HP-UX 10.20

HP HP-UX 11.00

HP HP-UX 11.11

IBM AIX 4.3

IBM AIX 5.1

* SGI IRIX 5.2-6.4

Compaq Tru64 DIGITAL UNIX v4.0f

Compaq Tru64 DIGITAL UNIX v4.0g

Securiteam: [UNIX] Multi-Vendor Format String Vulnerability in

Compaq Tru64 DIGITAL UNIX v5.0a

Compaq Tru64 DIGITAL UNIX v5.1

Compaq Tru64 DIGITAL UNIX v5.1a

* Sun Solaris 1.1–1.2

* Sun Solaris 2.0–2.7

Sun Solaris 7

Sun Solaris 8

* Note: This list is believed to be accurate, but not all platforms and versions have been tested. This list may or may not include every vulnerable platform and version.

Description:

The ToolTalk architecture is designed to allow custom applications to communicate with each other over the network. ToolTalk enabled applications communicate via RPC (Remote Procedure Call) and are managed by the ToolTalk database server (rpc.ttdbserverd). The rpc.ttdbserverd is enabled by default on many popular UNIX operating systems, even if its functionality is not needed or if ToolTalk enabled applications are not present.

ToolTalk contains a "syslog()" call that will interpret user-supplied formatting arguments. This call is insecure and allows remote attackers to control formatting and manipulate data at arbitrary locations in the memory of the running executable.

A format string vulnerability is similar to a buffer overflow vulnerability in that the result of a successful attack is unauthorized manipulation of protected memory in a running program. Format string vulnerabilities manifest when programmers neglect to specify a format argument when using functions in the "printf" family.

A secure print function may look like this:

```
printf(string, "%s");
```

A vulnerable print function may look like this:

```
printf(string);
```

When user-supplied strings encounter a printf function without a specified format argument, the string is printed without special formatting.

However, if a user creates a string including format characters and sends it to an insecure printf function, the string can function as a reference to memory that is normally out of bounds. In order to prevent this, printf functions must contain a print argument to securely restrict user-supplied input to specific memory locations.

Recommendations:

ISS X-Force recommends that all affected users apply the appropriate vendor-supplied patches listed below. X-Force also recommends that if ToolTalk is not explicitly required, it should be disabled immediately.

Securiteam: [UNIX] Multi-Vendor Format String Vulnerability in

Sun Microsystems, Inc.

Sun has reproduced the vulnerability and is testing a fix. The Sun patches will be made available at the following location:

<<http://sunsolve.sun.com/securitypatch>>

<http://sunsolve.sun.com/securitypatch>

Hewlett Packard, Inc.

All current HP-UX versions are vulnerable. HP has reproduced the vulnerability and has made an emergency fix available. HP customers should refer to HP Security Bulletin #0168 (Document ID HPSBUX0110-168) for more information. All HP security information is accessible at the following location:

<<http://www.itresourcecenter.hp.com/>> <http://www.itresourcecenter.hp.com/>

The HP emergency fix is now available at the following location: ftp site:

hprc.external.hp.com (192.170.19.51).

account: xgraphic

password: xgraphic

directory: ~xgraphic/CDE

file: rpc.ttdbserver.tar.gz

SGI

SGI is currently investigating the vulnerability and will announce a fix if one is made available. SGI security information is available at the following location:

<<http://www.sgi.com/support/security/>>

<http://www.sgi.com/support/security/>

Compaq Computer Corporation

Compaq has identified the vulnerability and made patches available. This patch may be obtained from the following URL address:

<<http://www.support.compaq.com/patches/>>

<http://www.support.compaq.com/patches/>

Select BROWSE PATCH TREE and choose the version directory required.

The patch names are:

DUV40F17-C0056200-11703-ER-*.tar

T64V40G17-C0007000-11704-ER-*.tar

T64V50A17-C0015500-11705-ER-*.tar

T64V5117-C0065200-11706-ER-*.tar

T64V51Assb-C0000800-11707-ER-*.tar

Note: The asterisk in the filename indicates the remainder of the tarfile name may change depending on the applicable date.

This patch can be installed on:

V4.0f, V4.0g all patch kits

V5.0a, V5.1, and V5.1a all patch kits

IBM Corporation

IBM has identified the vulnerability and will provide an emergency fix.

The fix will be made available from the following FTP site:

Securiteam: [UNIX] Multi-Vendor Format String Vulnerability in

<ftp://aix.software.ibm.com/aix/efixes/security/tooltalk_efix.tar.Z>
ftp://aix.software.ibm.com/aix/efixes/security/tooltalk_efix.tar.Z

ADDITIONAL INFORMATION

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Multiple Local Sendmail Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)