

[UNIX] HP Tru64 UNIX Running the ps command, Local Disclosure of Sensitive Information

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00010.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 7 May 2007 12:20:49 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

HP Tru64 UNIX Running the ps command, Local Disclosure of Sensitive Information

SUMMARY

A potential security vulnerability has been identified with the HP Tru64 UNIX Operating System running the ps command. The ps command could be used to disclose information about a process's arguments and environmental variables that might be exploited by a local, authorized user.

DETAILS

Vulnerable Systems:

- * HP Tru64 UNIX v5.1B-4
- * HP Tru64 UNIX v5.1B-3
- * HP Tru64 UNIX v5.1A PK6
- * HP Tru64 UNIX v4.0G PK4
- * HP Tru64 UNIX v4.0F PK8

HP has released the following Early Release Patch kits (ERPs) publicly for use by any customer.

The ERP kits use dupatch to install and will not install over any Customer

[UNIX] HP Tru64 UNIX Running the ps command, Local Disclosure of Sensitive Information

Specific Patches (CSPs) that have file intersections with the ERP.

The resolutions contained in the ERP kits are targeted for availability in the following mainstream patch kit:

HP Tru64 UNIX Version v5.1B-5

The ERP kits distribute the following files:

```
/usr/bin/ps  
/sbin/ps
```

After installing the patch kit, by default, the HP Tru64 UNIX ps command behaves just the same: it can display a process's arguments, and the ps e command displays a process's environmental variables.

To prevent users from seeing the arguments and environmental variables of other users, set new variables in the "/etc/rc.config.common" file (versions v5.1A PK6, v5.1B-3, v5.2B-4) or the "/etc/rc.config" file (versions v4.0G PK4 and v4.0F PK8) as follows:

For HP Tru64 UNIX versions v5.1B-4, v5.1B-3 and v5.1A PK6, use:

```
# rcmgr -c set TBL_ARGUMENTS_DISABLE 1  
# rcmgr -c set TBL_ENVIRONMENT_DISABLE 1
```

For HP Tru64 UNIX versions v4.0G PK4 and v4.0F PK8, use:

```
# rcmgr set TBL_ARGUMENTS_DISABLE 1  
# rcmgr set TBL_ENVIRONMENT_DISABLE 1
```

Setting the new variables to prevent the ps command from allowing non-root users to display other users arguments and environment variables might cause some applications or program scripts to not function properly. The root user running the ps command will continue to be allowed to display other users arguments and environment variables.

HP Tru64 UNIX Version v5.1B-4 ERP Kit:

Location:

<<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001143-V51BB27-ES-20070305>>
<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001143-V51BB27-ES-20070305>

Name: T64KIT1001143-V51BB27-ES-20070305

MD5 Checksum: 44b15d10895cf0606003a572b3310f9a

HP Tru64 UNIX Version v5.1B-3 ERP Kit:

Location:

<<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001144-V51BB26-ES-20070305>>
<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001144-V51BB26-ES-20070305>

Name: T64KIT1001144-V51BB26-ES-20070305

MD5 Checksum: 67cfabb7cd3c422e2dc6bb6ed3d7d290

HP Tru64 UNIX Version v5.1A PK6 ERP Kit:

Location:

<<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001145-V51AB24-ES-20070305>>

[UNIX] HP Tru64 UNIX Running the ps command, Local Disclosure of Sensitive Information

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001145-V51AB24-ES-20070305>

Name: T64KIT1001145-V51AB24-ES-20070305

MD5 Checksum: de6885b166dba703af862ce05431e5cc

HP Tru64 UNIX Version v4.0G PK4 ERP Kit:

Location:

<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=T64KIT1001179-V40GB22-ES-20070330>

Name: T64KIT1001179-V40GB22-ES-20070330

MD5 Checksum: 31129e60bb01ffdea015312c0e019fae

HP Tru64 UNIX Version v4.0F PK8 ERP Kit:

Location:

<<http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1001180-V40FB22-ES-20070330>

> <http://www.itrc.hp.com/service/patch/patchDetail.do?patchid=DUXKIT1001180-V40FB22-ES-20070330>

Name: DUXKIT1001180-V40FB22-ES-20070330

MD5 Checksum: db9d634bb27f02642e00f149d6ebb8ee

ADDITIONAL INFORMATION

The information has been provided by HP Software Security Response Team.

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.