

[UNIX] HP Ignite-UX Information Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/05

To: list@securiteam.com

Date: 18 Aug 2005 16:55:46 +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 Ignite-UX Information Disclosure

SUMMARY

"The <<http://www.docs.hp.com/en/IUX/index.html>> HP Ignite-UX application addresses the need for HP-UX system administrators to perform system installations and deployment, often on a large scale"

A vulnerability in HP Ignite-UX allows anonymous users to access the operating system's password file.

DETAILS

Vulnerable Systems:

- * HP Ignite-UX prior to version C.6.2.240 and prior

Immune Systems:

- * HP Ignite-UX version C.6.2.241 or newer

The HP Ignite-UX can use a TFTP server to facilitate anonymous access to configuration data. When the `make_recovery` command is used, a copy of the `/etc/passwd` file will be created in the TFTP server tree and made available for anonymous access.

As of version B.3.2 of the product, the `make_recovery` command has been

Securiteam: [UNIX] HP Ignite-UX Information Disclosure

depreciated in preference for the make_tape_recovery command (which doesn't display the same issues), and as of version C.6.0 the make_recovery command does not exist in the product at all. However, if at any point make_recovery has been run on the host, a copy of the /etc/passwd file may still remain within the TFTP server tree.

Proof of Concept:

Use a TFTP client to request the file referenced by the following path:
/var/opt/ignite/recovery/passwd.makrec

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0951>>
CAN-2004-0951

Disclosure Timeline:

Discovered: 23.11.04 (Martin O'Neal)
Vendor notified: 23.11.04
Document released: 16.08.05

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@corsaire.com>>
Corsaire.

The original article can be found at:
<<http://www.corsaire.com/advisories/c041123-001.txt>>
<http://www.corsaire.com/advisories/c041123-001.txt>

=====

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.