

NISCC Vulnerability Advisory 688910/NISCC/IGNITE-UX

Vulnerability Issues with HP Ignite-UX

Version Information

Advisory Reference	688910/NISCC/IGNITE-UX
Release Date	16 August 2005
Last Revision	16 August 2005
Version Number	1.0

Acknowledgement

These issues were identified by Corsaire Ltd, a privately owned UK company.

What is Affected?

The following versions are affected:

- HP-UX B.11.00 running Ignite-UX
- HP-UX B.11.11 running Ignite-UX
- HP-UX B.11.22 running Ignite-UX
- HP-UX B.11.23 running Ignite-UX

Impact

If exploited, these vulnerabilities can result in unintended information disclosure and possible denial-of-service.

Severity

The is rated as low.

Summary

Ignite-UX is an HP-UX administration toolset to help users:

- Install HP-UX on multiple systems in their network
- Create custom install configurations
- Recover HP-UX systems remotely

- Monitor system-installation status

Several vulnerabilities concerning the HP Ignite-UX product were discovered by Corsaire Ltd. These vulnerabilities arise from the TFTP server embedded in Ignite-UX; the TFTP server is used by Ignite-UX to facilitate anonymous access to its configuration data.

HP has addressed the problems and has solutions available to rectify the flaws. Please see the 'Solution' section for further details.

Details

As part of the installation process, HP Ignite-UX can install and enable a TFTP server to facilitate anonymous access to configuration data. It is with this service that the following vulnerabilities arise from.

However please note that several factors must be correct to take advantage of these vulnerabilities remotely:

- This only affects machines that are running certain version of HP-UX
- These affected machines have the TFTP server running
- The TFTP server is accessible externally
- A specific command is executed

*151204/NISCC/IGNITE-UX/1
CVE ID: CAN-2004-0952*

In certain circumstances when the `add_new_client` command is used, some sections of the TFTP server tree can become world-writable. This can allow a malicious person to use it as a mechanism for moving objects into and out of the system, or simply launch a denial-of-service attack against the host by filling up the local filesystem.

*151204/NISCC/IGNITE-UX/2
CVE ID: CAN-2004-0951*

In certain circumstances 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.

However please note that as of version B.3.2 of the product, the `make_recovery` command has been deprecated in preference for the `make_tape_recovery` command; also as of version C.6.0 of the product, the `make_recovery` command does not exist at all. But please bear in mind that if at any point the `make_recovery` command has been executed on the host, then a copy of the `/etc/passwd` file may still exist within the TFTP server tree.

Mitigation

To minimise the risk of these vulnerabilities, we suggest the following:

- If the TFTP server is not required, the please ensure that it is disabled.
- If the TFTP server is required, then please ensure that the TFTP server is not available externally; as a general security practice, TFTP traffic should be blocked at the network gateway.

Solution

HP has made the following available to resolve the issue:

- `Ignite-UX-11-00_C.6.2.241_HP-UX_B.11.00_32+64.depot`
- `Ignite-UX-11-11_C.6.2.241_HP-UX_B.11.00_32+64.depot`
- `Ignite-IA-11-22_C.6.2.241_HP-UX_B.11.00_32+64.depot`
- `Ignite-UX-11-23_C.6.2.241_HP-UX_B.11.00_32+64.depot`

These updates are available on <http://www.hp.com/go/softwaredepot> (search for IGNITEUXB).

Vendor Information

Hewlett-Packard is a technology solutions provider to consumers, businesses and institutions globally. The company's offerings span IT infrastructure, global services, business and home computing, and imaging and printing.

For more information regarding Hewlett-Packard, please visit <http://www.hp.com/>.

Credits

This issue was discovered by Corsaire Ltd, who reported the issue to NISCC. The NISCC Vulnerability Team would also like to thank HP for their co-operation in the handling of this vulnerability.

Contact Information

The NISCC Vulnerability Management Team can be contacted as follows:

Email	vulteam@nisc.gov.uk <i>(Please quote the advisory reference in the subject line.)</i>
Telephone	+44 (0)870 487 0748 Extension 4511 <i>(Monday to Friday 08:30 - 17:00)</i>
Fax	+44 (0)870 487 0749
Post	Vulnerability Management Team NISCC PO Box 832 London SW1P 1BG

We encourage those who wish to communicate via email to make use of our PGP key. This is available from <http://www.nisc.gov.uk/nisc/publicKey2-en.pop>.

Please note that UK government protectively marked material should not be sent to the email address above.

If you wish to be added to our email distribution list, please email your request to uniras@nisc.gov.uk.

What is NISCC?

For further information regarding the UK National Infrastructure Security Co-Ordination Centre, please visit the NISCC web site at: <http://www.nisc.gov.uk/>

Reference to any specific commercial product, process or service by trade name, trademark manufacturer or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

Neither shall NISCC accept responsibility for any errors or omissions contained within this advisory. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

© 2005 Crown Copyright

Revision History

16 August 2005 Initial release (1.0)

<End of NISCC Vulnerability Advisory>