

[NEWS] ChaiVM Multiple Security Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0121.html>

From: support@securiteam.com

Date: 07/28/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 28 Jul 2002 08:06:00 +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.

ChaiVM Multiple Security Vulnerabilities

SUMMARY

<<http://www.hp.com/products1/embedded/products/platform/chaivm.html>>

ChaiVM is used in networked appliances such as printers, mobile computing devices, and other mobile or fixed networked embedded hardware. Two security vulnerabilities in the product have been found allowing any network user to add additional Chai Services to the product (compromising the security of the product).

DETAILS

Vulnerable systems:

- * Hewlett Packard (HP) ChaiVM
- * HP 9000
- * HP 4100
- * HP 45nn
- * HP 8150

(Possibly others using ChaiVM)

HP Bug ID:

Not assigned

CERT Vulnerability ID:

780747

Securiteam: [NEWS] ChaiVM Multiple Security Vulnerabilities

Two vulnerabilities exist.

1. Access to the file system hosting ChaiVM will allow any user to add, delete, or modify services hosted by the ChaiServer. This is especially applicable in cases where the file is accessible through the network using PJJ (Printer Job Language).
2. The default loader (this.loader) verifies JAR signatures. However, HP released an advanced loader (EZloader, this.ez), which in turn, does not verify signatures for new services.

Vendor status:

06/29/02 Initial Notification, security-alert@hp.com *Note-Initial notification by phenoelit includes a cc to cert@cert.org by default
06/29/02 RBL blocked delivery to security-alert@hp.com
06/29/02 Creation of ho-mail account and retransmission
06/29/02 Auto-responder reply
07/01/02 Human contact, PGP exchange and acknowledge.
07/01/02 Clarification of some details w/HP Sec people
07/19/02 Notification of intent to post publicly in approximately 7 days.
07/23/02 Coordination for release date/times

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fx@phenoelit.de>> FX, <<mailto:ftR@phenoelit.de>> FtR, <<mailto:kim0@phenoelit.de>> kim0, and <<mailto:DasIch@phenoelit.de>> DasIch.

=====

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: "[EXPL] IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)