

SSRT3632 HP Software Security Customer Advisory

Information as of October 13, 2003

SSRT3632 HP Web Management Software Security Vulnerability

Summary

HP Management Software products undergo rigorous quality assurance processes to ensure that they meet the highest possible standards for security, reliability and usability. In line with this commitment, a security vulnerability was recently uncovered in the non-SSL web agent (CPQHMMO.DLL version 3.7 and below) that is delivered as part of the HP web-enabled Management Software for desktops, notebooks, and workstations. This vulnerability has the potential to enable unauthorized users to execute code at an administrator level through the exploitation of a buffer overflow, allow a remote user to determine if a specified file on the system exists, and to the ability for a remote user to stop the HP web management services.

HP strongly recommends that customers remove the appropriate versions of web-enabled agents. This HP Customer Advisory will be updated as needed to communicate availability of new versions or changes to the affected products.

HP strongly recommends that web-enabled agents and utilities be deployed only on private networks and are not used on the open Internet or on systems outside the bounds of a firewall. The implementation of sound security practices, which includes disabling external access to HP management ports should help to protect customers from external malicious attacks. HP also recommends that strong password standards are used and that passwords are changed regularly.

Scope of the Problem

The web component of HP web-enabled management software provides HTTP services to allow management information to be accessible through a web browser. Web-enabled management software is preinstalled and provided for the majority of the operating systems that HP supports.

This Customer Advisory applies specifically and only to software named in the accompanying table. You may or may not have in use in your environment other software from HP that may or may not exhibit this condition but is not covered in this advisory.

What HP Is Doing

Insight Management Agent version 5.01 Rev A (SP24815.[EXE](#) / [TXT](#)) default install process was changed to not install the web portion of the agent and to also disable the Remote Diagnostics Enabling Agent (RDEA). RDEA also includes a web agent. Selecting 'custom install' will still allow the web agent to be selected and installed. This HP Customer Advisory will be updated as needed to communicate availability and plans for new versions the affected software. You may sign up for automatic notification of drivers and alerts at <http://h30046.www3.hp.com/subhub.php> (select 'driver & support alerts/notifications' then Servers/HP Server Management Software/HP Management Applications) but it is recommended that you check back here for new information periodically and not wait for notifications.

What Customers Should Do

- 1) Determine which systems are running HP web-enabled agents or utilities
- 2) Disable the web agent on those systems.

1) Determine which systems are running HP web-enabled agents or utilities. There are three methods suggested.

Method 1

Environments running Insight Manager 7 can get a list of systems running the web-enabled agents by defining a Query to return a list of systems with web agents.

Login to your Insight Manager 7 system and create a new Query. Select the "Devices with Web Agent" criteria.

- Select all of the available products on the Criteria Configuration screen.

- Save the Query and execute it. The list of devices will be all those with web agents. You may wish to use this query with the Reports feature of Insight Manager 7 (available in SP1 and greater) to get printouts of the devices and the software loaded. (Insight Manager XE users may follow a similar procedure up to but not including the reports.)

NOTE: Prior to running through this procedure, you may want to perform a new discovery and data collection. If you first make sure that the discovery range covers all of the subnets visible to the Insight Manager 7 system, you will get a potentially more comprehensive report.

Method 2

Systems running HP Insight Manager Windows 32 console, can get a list of systems running the web agents by starting HP Insight Manager and selecting the "Web Device List" button on the toolbar. This will display a list of systems being managed by HP Insight Manager and additionally will have underlined as hyperlinks the systems on which the web agents are present and enabled. To print out a list of only the web devices, select the "Web Devices" hyperlink in the left column and only web devices will be shown. Print this page from your browser.

NOTE: The lists generated by Methods 1 and 2, while helpful, may not be exhaustive lists of the systems with web-enabled agents and utilities. The lists will include only those systems that are being managed either explicitly or because they have been discovered.

Method 3

Point a web browser to the system by keying in [http://\[IP_ADDRESS\]:2301](http://[IP_ADDRESS]:2301) or [http://\[machine_name\]:2301](http://[machine_name]:2301).

This will bring up the device home page for any servers running web-enabled management software. This procedure identifies the presence of the software on 1 system and assumes that you already know the device name or IP address of every device and use this procedure to visit them.

2) In order to minimize the risk of your systems due to a malicious attack, HP recommends uninstalling or disabling the web agent software. To stop the relevant client services, use the NET STOP command on the following services: CpqWebDmi, DfwWebAgent, and LCRMS. To disable the services change the appropriate registry service "start" value to 4 as shown below:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CpqWebDmi]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DfwWebAgent]
"Start"=dword:00000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LCRMS]
"Start"=dword:00000004

Version/Platform/Operating System Matrix [follows]

HP AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS AND/OR SOFTWARE PUBLISHED ON THIS SERVER FOR ANY PURPOSE. ALL SUCH DOCUMENTS AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND AND ARE SUBJECT TO CHANGE WITHOUT NOTICE. THE ENTIRE RISK ARISING OUT OF THEIR USE REMAINS WITH THE RECIPIENT. IN NO EVENT SHALL HP AND/OR ITS RESPECTIVE SUPPLIERS BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION), EVEN IF HP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Agent /Utility	Platform	Operating System	Versions affected	Product Version Fixed / Download #
Insight Management for Clients	Desktops, Notebooks, Workstations	Windows 9x, NT 4.0, 2000, and XP.	3.50 - 5.00k	Product is going end-of-life December 31, 2003.
Remote Diagnostics Enabling Agent	Desktops, Notebooks, Workstations	Windows 9x, NT 4.0, 2000, and XP.		Product is going end-of-life December 31, 2003.
Insight Manager LC	Desktops, Notebooks, Workstations	Windows 9x, NT 4.0, and 2000.	1.00 – 1.60	Product went end-of-life October 2001.