HP ProLiant Essentials Vulnerability and Patch Management Pack Release Notes

Version

Version: 2.0.1

Supported platforms

For information about supported platforms and system prerequisites, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix* located on the HP Management CD or HP Insight Control Data Center Edition DVD.

What's new in version 2.0.1

- The Vulnerability and Patch Management Pack 2.0.1 resolves some existing issues with the installer and uninstaller.
- The English version of the Vulnerability and Patch Management Pack can now be installed on a Japanese operating system. Scanning and patching Japanese targets is also supported. Information about Japanese support can be found at **http://www.hp.com/jp/servers/vpm**.

  NOTE: Kanji characters cannot be used in passwords, directories, or scan names.

What's new in version 2.00

- The Vulnerability and Patch Management Pack 2.00 is a required upgrade for current users. The installer for the Vulnerability and Patch Management 2.00 completes a fresh installation or upgrades previous versions. All users are required to run a full patch acquisition to update the patch database and download the latest VPM patch agent.

  Microsoft® recently introduced the Microsoft Update Catalog, a centralized repository for all Microsoft patches. Patches for new products introduced by Microsoft are only available through this new repository. Because of this change, the Vulnerability and Patch Management Pack has adopted this new repository as a source for the patches being provided by Microsoft.
- HP Systems Insight Manager (HP SIM) 5.0 SP2 or later is supported. To download the latest patch or HP SIM installation, see **http://www.hp.com/go/hpsim**.
- New patch installation status reports are available. Gain new insight with status reports created by patch, system, or search filter (advisory, system, or patch status).
- Microsoft SQL Server database is supported. To use a SQL Server database, the database must be installed before installing or upgrading the Vulnerability and Patch Management Pack. Users upgrading from a previous version of the Vulnerability and Patch Management Pack have the option to switch database types.

Changes in version 2.0.1

- The Radia Management Agent (RMA) has been updated to eliminate potential to hang on some target systems or the HP SIM Central Management Server (CMS) when they are rebooted. If you disabled the RMA service on a target system as a workaround, you can redeploy the VPM Patch Agent or reset the server to start automatically after you have installed the Vulnerability and Patch Management Pack 2.0.1. The next patching session for the target system automatically updates the RMA service.
- The installer allows passwords with spaces.
- The uninstaller stops all services using SNMP to remove the EDMSNMPX.DLL file.
- The missing license.nvd file is included in the VPM Acquisition Utility.

Changes in version 2.00

- Support is available for the new Microsoft patch repository, Microsoft Update Catalog. The patch acquisition process using the Vulnerability and Patch Management Pack remains unchanged.
- Microsoft Windows NT® 4.0 patch acquisitions are no longer supported.
- The link for obtaining Harris STAT® Scanner updates has changed. If your firewall is configured for access to HP, change your firewall access to allow **https://ftp.hp.com/pub/essentials/vpm** to ensure that the Vulnerability and Patch Management Pack can successfully continue to obtain updates.
- Some advisories are listed as MS-KB*xxxxx*. This new naming convention is for security rollups, bundled patches which are not considered service packs. The Vulnerability and Patch Management Pack now supports distribution and management of these security rollups.

Installation notes

1. For information about installation and setup of the Vulnerability and Patch Management Pack, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster* and the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
2. Microsoft Internet Information Server (IIS) 5.0 or later must be installed and running on the VPM server, the server on which the Vulnerability and Patch Management Pack is installed. For information about configuring a secure HTTPS connection between the Vulnerability and Patch Management Pack and HP SIM, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide* and **http://support.microsoft.com/?kbid=324069**.

   NOTE: HP recommends an HTTPS connection when the Vulnerability and Patch Management Pack and HP SIM are installed on separate servers.
3. HP SIM 5.0 SP2 or later and WMI Mapper must be installed and running before installing the Vulnerability and Patch Management Pack. HP SIM is available at **http://www.hp.com/go/hpsim**.
4. The Vulnerability and Patch Management Pack must be installed using an account password that does not contain curly braces, ("{" or "}"). To change the installation account password before installing the Vulnerability and Patch Management Pack, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
5. If a version of Microsoft Data Access Components (MDAC) earlier than 2.5 SP1 is loaded on the VPM server, MDAC 2.5 SP1 is automatically installed and the system is rebooted. The Vulnerability and Patch Management Pack installation must be restarted.
6. HP SIM is restarted at the completion of the Vulnerability and Patch Management Pack installation or uninstallation.
7. SNMP service must be started on the HP SIM system to facilitate the HP SIM discovery and identification of target systems.

Other environment setup requirements

1. If the target systems, the systems to be managed by HP SIM and the Vulnerability and Patch Management Pack, are not defined in a DNS server, complete the following steps before installing HP SIM to allow HP SIM to correctly discover and identify these systems.
   - Update the hosts file (located at C:\%system%\drivers\etc on the HP SIM server) with the IP address, short name, and full name of these systems.
   - Configure the primary DNS suffix.
   - Include the VPM server if the Vulnerability and Patch Management Pack is installed on a separate server than HP SIM.
2. Microsoft Internet Explorer 6.0 or later must be used to access HP SIM. Adobe® Reader 3.*x* or later must be installed on the system used to view vulnerability scan results. To view the scan result .pdf files, validate the following browser settings:
   - Internet Access Security is set to **Medium.**
   - Under Advanced Options, the **Do not save encrypted pages to disk** checkbox is **not** selected.
3. If the VPM server is inside a firewall and patches will be acquired from the VPM server, the firewall must allow FTP and HTTP to successfully perform the patch acquisitions.

   If the VPM server does not have Internet access or the firewall blocks either FTP or HTTP communication, the VPM Acquisition Utility can be used on a separate system to acquire patches. The system on which the VPM Acquisition Utility is installed must have Internet access, and the firewall must allow FTP or HTTP communications.

   Upgrade the VPM Acquisition Utility when the Vulnerability and Patch Management Pack is upgraded.
4. If Microsoft Windows® XP systems not joined to a Windows domain are target systems in a vulnerability scan or patch-fix operation, Simple File Sharing must be disabled on those systems for these scanning/patching functions to be successful. For more information, see **http://support.microsoft.com/default.aspx?scid=kb;EN-US;q304040**.
5. Windows XP systems with Service Pack 2 installed which are used as target systems in a patch-fix operation must place the RADEXECD and NVDKIT programs on the firewall exception list. These programs open sockets that must be accessible to deploy patches.
6. When scanning a target system that is a domain controller, be sure that the credentials for accessing that system include the domain name and user name since there are no local accounts on a domain controller.
7. A subscription to the Red Hat Network and additional setup procedures are required to acquire patches from the Red Hat Network. To successfully deploy patches to Red Hat Linux target systems, a systemid file must be created for each version of Red Hat patches and a required library must be installed on the target systems. For information, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
8. The Vulnerability and Patch Management Pack allows credentials with administrator-level privileges to access remote systems. In some environments, it might be possible to spoof a remote system causing a "man-in-the-middle-attack." In a Windows environment, stealing the credentials used to access a remote system is highly unlikely because Windows authentication uses a one-way hashing function to encrypt the credentials. In a Linux environment, SSH provides a similar mechanism over an encrypted communications channel. For additional information about configuring HP SIM SSL and SSH features for use with the HP Insight Management Agents, see the HP SIM documentation at **http://www.hp.com/go/hpsim**.
9. Red Hat Enterprise Linux 3 automatically configures a firewall when installed. To patch these systems the firewall must be disabled by executing setup to launch the user interface on the target system and disabling the firewall from the user interface.

Important notes

- For information about setting up credentials to access the target systems, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster*. Scanning and patching target systems require administrator-level access.
- The VPM Patch Agent is automatically deployed when a target system is first licensed. If the system is not accessible or the credentials are not set up correctly, the VPM Patch Agent might not be installed. You can verify the installation by viewing the VPM events listed in the HP SIM event log. If necessary, manually install the VPM Patch Agent after correcting the credentials by selecting **Deploy>Vulnerability and Patch Management>VPM Patch Agent.**
- To use the Vulnerability and Patch Management Pack immediately, you might want to select only one operating system the first time patches are acquired to minimize acquisition time. The acquisition of the first operating system and scan definitions can take approximately two hours. A patch acquisition of every operating system can take four to six hours to complete the first time the acquisition is run. The start of the patch acquisition event is displayed in the HP SIM event log.
- If you use a proxy in your environment, be sure to set up the proxy settings before using the Vulnerability and Patch Management Pack to acquire updates. Set up the proxy settings by selecting **Options>Vulnerability and Patch Management>Settings.**

Limitations and known issues in version 2.00

- The following message is written to the Windows Event Log occasionally when the Harris STAT Scanner components are updated during a patch acquisition operation:

  ```
  Application popup w3wp.exe - Application Error: The instruction at
  0x7c82f350 referenced memory at 0x02bf0824. The memory could not be
  written.
  ```

  This error can be ignored. The STAT component w3wp.exe sometimes ends abnormally when a new version is put into place.
- Patch acquisitions can generate events containing HTTP 300 errors for some older Microsoft patches. For example:

  ```
  Error downloading patch data for Bulletin MS02-050 at URL
  http://www.microsoft.com/ntserver/terminalserver/downloads/critical/
  q329115/default.asp error code 300
  ```

  HP is working to correct the metadata for these older patches. However, this maintenance is ongoing.
- If an HP SIM discovery or identification task is in progress when target systems are licensed for the Vulnerability and Patch Management Pack, target systems that have an IP address as their name at the time of licensing that are later identified with a system name might become unlicensed and have to be licensed again. Avoid this situation by allowing discovery and identification tasks to complete before licensing the target systems. Another alternative is to complete the following steps to properly set up the name in HP SIM for the target systems:
  a. Display the **All Systems** list.
  b. Double-click the node name to display its system page.
  c. Click the **Links** tab.
  d. Select **Edit System Properties.**
  e. Enter the desired system name in the preferred system name field.
  f. Click **OK.**
- When a SQL Server database is used, the Vulnerability and Patch Management Pack database credentials are not updated by the Change VPM Credentials utility. There is currently not a supported method for changing the credentials manually. An engineering advisory will be issued at a later time with instructions to change the database credentials.

- When licensing a VMware system with a serial number longer than 30 characters, a limitation in the HP SIM License Manager causes the VPM license to function incorrectly on this system, as well as any other HP SIM node licensed by serial number. The VMware target host is continually considered "unlicensed," and must be relicensed each time the system is selected for a licensed operation. This issue will be resolved in a future release of HP SIM.
- Systems in private collections cannot be scanned. A .dat file cannot be selected, and the following message is displayed:
  `There are no licensed nodes.`
- Some systems might be incorrectly identified and appear capable of being licensed in both the VPM column and licensing pages. Before applying a license to a system, be sure the system is supported by referring to the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*.
- Some Microsoft patches, such as MS04-025, do not appear in the Control Panel after being installed. To verify installation, run the vulnerability scan again.
- Microsoft Windows File Protection maintains backup copies of critical system files in a hidden directory named "dllcache" so that these critical files can be replaced if they are removed for any reason. Uninstalling an application can remove some of these critical files. In rare situations, you might be prompted to insert the installation media into a system when a patch is being installed and a backup file is missing or corrupted. This condition can also occur when installing software other than patches.
- The installation fails if curly braces, ("{" or "}") are used in the account password used to install the Vulnerability and Patch Management Pack. The account password must be changed to remove those characters before installation. The password can be changed back to the original password after the Vulnerability and Patch Management Pack installation is complete. For details, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
- A generic Radia internal error appears in the HP SIM event log if the patch repository is viewed before a patch acquisition is performed.
- Resolutions for some fixable vulnerabilities cause the local security policy to log more events. If the logs are configured not to overwrite old events, the event log can become full and cause abnormal system behavior. Read and understand the effects of all fixes before applying them.
- Acquiring patches from the Red Hat Network requires the network connection to remain connected for the duration of the acquisition operation. If the network goes down, the patch acquisition must be restarted.
- If a group of systems is selected to receive configuration fixes and some systems in that group do not require all the fixes, the fix events are still displayed for those systems. However, the Vulnerability and Patch Management Pack does not actually apply the fixes to those systems that do not require them.
- If a patch causes a reboot when patching the system on which HP SIM is running, the **Diagnose>Vulnerability and Patch Management>View patch installation status>View Patches Installed by VPM** list might continue to indicate Reboot Required. Select **Deploy>Vulnerability and Patch Management>Validate Install Patches** to update the installed patches list.
- If multiple systems are scanned as a group and many vulnerabilities exist, the Scan Detail report for the group might be too large to be generated. View the Scan Detail report for individual systems in the group.
- If a system has a Microsoft service pack installed that is not the final release, patches applied to that system might return the status "Not Applicable." Only official releases of service packs should be installed on a system being scanned and patched by the Vulnerability and Patch Management Pack.
- Applying more than 100 patches in a single operation can cause a timeout to occur. HP recommends installing less than 100 patches at a time.

- The Back button in the Internet Explorer web browser does not function properly. Use navigation buttons within the HP SIM and Vulnerability and Patch Management Pack pages.
- If a secure connection is configured between the Vulnerability and Patch Management Pack and HP SIM by installing an IIS certificate, scanning no longer works if the certificate is later removed. To continue without renewing the certificate, uninstall and reinstall the Vulnerability and Patch Management Pack.
- Patches that have been superseded will not be acquired. If you apply a patch that has been superseded, the superseding patch is applied instead.
- The single quote character, "'," cannot be used as part of a user-assigned vulnerability scan name. If this character is used, the scan report is not generated.

For more information

- http://www.hp.com/go/vpm
- *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*
- *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*
- *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster*

June 2006