

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [bugtraq](#)
Subject: [security bulletin] HPSBST02386 SSRT080164 rev.1 - Storage Management Appliance (SMA), Mic
From: [security-alert\(.\)hp!com](#)
Date: [2008-11-18 13:41:46](#)
Message-ID: [20081118134147.A426BBC93\(.\)hpchs!cup!hp!com](#)
[Download RAW [message](#) or [body](#)]

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c01606691
Version: 1

HPSBST02386 SSRT080164 rev.1 - Storage Management Appliance (SMA), Microsoft Patch \ Applicability MS08-067 to MS08-069

NOTICE: The information in this Security Bulletin should be acted upon as soon as \ possible.

Release Date: 2008-11-17
Last Updated: 2008-11-17

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Various potential security vulnerabilities have been identified in Microsoft software \ that is running on the Storage Management Appliance (SMA). Some of these \ vulnerabilities may be pertinent to the SMA, please check the table in the Resolution \ section of this Security Bulletin.

References: MS08-067 (CVE-2008-4250),
MS08-068 (CVE-2008-4037),
MS08-069 (CVE-2007-0099, CVE-2008-4029, CVE-2008-4033)

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
Storage Management Appliance v2.1 Software running on:

Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
--	Not Applicable	--

Information on CVSS is documented in HP Customer Notice: HPSN-2008-002.

Patches released by Microsoft after MS06-051 are covered by monthly Security \ Bulletins.

For the full archived list of Microsoft security updates applicable for Storage \ Management Appliance software v2.1, please refer to the following Security Bulletins \ available on the IT Resource Center (ITRC) Web site: \ <http://www.itrc.hp.com/service/cki/secBullArchive.do>

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security \ Bulletin HPSBST02146 For patches released by Microsoft in 2004, MS04-001 to MS04-045 \ refer to Security Bulletin HPSBST02147 For patches released by Microsoft in 2005, \ MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148 For patches released by \ Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140

The Microsoft patch index archive and further details about all Microsoft patches can \ be found on the following Web site: \ <http://www.microsoft.com/technet/security/bulletin/summary.msp>

Note: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for \

Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 \ Update Rollup 1 for Service Pack 4 and Storage Management Appliance v2.1 advisory at \ the following website: \ <http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=Support \ Manual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=12169&prodSeriesId=315667 \>

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after \ April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and \ MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 \ for SP4, if they have not been installed already

RESOLUTION

HP strongly recommends the immediate installation of all security patches that apply \ to third party software which is integrated with SMA software products supplied by \ HP, and that patches are applied in accordance with an appropriate patch management \ policy.

Note: Patch installation instructions are shown at the end of this table.

MS Patch - MS08-067 Vulnerability in Server Service Could Allow Remote Code Execution \ (958644) Analysis - Possible security issue exists. Patch will run successfully.
Action - For SMA v2.1, customers should download patch from Microsoft and install.

MS Patch - MS08-068 Vulnerability in SMB Could Allow Remote Code Execution (957097)
Analysis - Possible security issue exists. Patch will run successfully.
Action - For SMA v2.1, customers should download patch from Microsoft and install.

MS Patch - MS08-069 Vulnerabilities in Microsoft XML Core Services Could Allow Remote \ Code Execution (955218) Analysis - Possible security issue exists. Patch will run \ successfully. Action - For SMA v2.1, customers should download patch from Microsoft \ and install.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA
Copy the patch to a floppy diskette or to a CD
Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, \ monitor and mouse to the SMA.

Note: The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more \ information please refer at the following website: \ <http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&display1>

PRODUCT SPECIFIC INFORMATION

None

HISTORY

Version:1 (rev.1) - 17 November 2008 Initial release

Third Party Security Patches: Third party security patches that are to be installed \ on systems running HP software products should be applied in accordance with the \ customer's patch management policy.

Support: For further information, contact normal HP Services support channel.

Report: To report a potential security vulnerability with any HP supported product, \ send Email to: security-alert@hp.com It is strongly recommended that security \ related information being communicated to HP be encrypted using PGP, especially \ exploit information. To get the security-alert PGP key, please send an e-mail \ message as follows:

To: security-alert@hp.com
Subject: get key

Subscribe: To initiate a subscription to receive future HP Security Bulletins via \ Email: [http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in_SC-GEN_driverITRC&](http://h30046.www3.hp.com/driverAlertProfile.php?regioncode=NA&langcode=USENG&jumpid=in_SC-GEN_driverITRC&On the web page: ITRC security bulletins and patch sign-up)
On the web page: ITRC security bulletins and patch sign-up
Under Step1: your ITRC security bulletins and patches
- check ALL categories for which alerts are required and continue.
Under Step2: your ITRC operating systems
- verify your operating system selections are checked and save.

To update an existing subscription: <http://h30046.www3.hp.com/subSignIn.php>
Log in on the web page: Subscriber's choice for Business: sign-in.

On the web page: Subscriber's Choice: your profile summary - use Edit Profile to \ update appropriate sections.

To review previously published Security Bulletins visit: \ <http://www.itrc.hp.com/service/cki/secBullArchive.do>

* The Software Product Category that this Security Bulletin relates to is represented \ by the 5th and 6th characters of the Bulletin number in the title:

GN = HP General SW
MA = HP Management Agents
MI = Misc. 3rd Party SW
MP = HP MPE/iX
NS = HP NonStop Servers
OV = HP OpenVMS
PI = HP Printing & Imaging
ST = HP Storage SW
TL = HP Trusted Linux
TU = HP Tru64 UNIX
UX = HP-UX
VV = HP VirtualVault

System management and security procedures must be reviewed frequently to maintain \ system integrity. HP is continually reviewing and enhancing the security features of \ software products to provide customers with current secure solutions.

"HP is broadly distributing this Security Bulletin in order to bring to the attention \ of users of the affected HP products the important security information contained in \ this Bulletin. HP recommends that all users determine the applicability of this \ information to their individual situations and take appropriate action. HP does not \ warrant that this information is necessarily accurate or complete for all user \ situations and, consequently, HP will not be responsible for any damages resulting \ from user's use or disregard of the information provided in this Bulletin. To the \ extent permitted by law, HP disclaims all warranties, either express or implied, \ including the warranties of merchantability and fitness for a particular purpose, \ title and non-infringement."

©Copyright 2008 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company shall not be liable for technical or editorial errors or \ omissions contained herein. The information provided is provided "as is" without \ warranty of any kind. To the extent permitted by law, neither HP or its affiliates, \ subcontractors or suppliers will be liable for incidental, special or consequential \ damages including downtime cost; lost profits; damages relating to the procurement of \ substitute products or services; or damages for loss of data, or software \ restoration. The information in this document is subject to change without notice. \ Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein \ are trademarks of Hewlett-Packard Company in the United States and other countries. \ Other product and company names mentioned herein may be trademarks of their \ respective owners.

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1

iQA/AwUBSSH8uAf0vwtKn1ZEQJ7TQCfUEM8pQm8GZsAoeZaKuFpKNEnCB4Ao0jg
CS3Wc508RMURAIstlnvjvBTv
=I5HK

-----END PGP SIGNATURE-----

[[prev in list](#)] [[next in list](#)] [[prev in thread](#)] [[next in thread](#)]

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)