

[security bulletin] HPSBGN02319 SSRT080027 rev.1 – HP Compaq Notebook PC BIOS, Local Unauthorized Access

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00373.html>

- *From:* security-alert@xxxxxx
 - *Date:* Fri, 28 Mar 2008 06:03:32 -0700
-

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

Hash: SHA1

SUPPORT COMMUNICATION – SECURITY BULLETIN

Document ID: c01393763

Version: 1

HPSBGN02319 SSRT080027 rev.1 – HP Compaq Notebook PC BIOS, Local Unauthorized Access

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

Release Date: 2008-03-27

Last Updated: 2008-03-27

Potential Security Impact: Local Unauthorized Access

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

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP Compaq Notebook PC BIOS. The vulnerability could be exploited to allow local unauthorized users access to the system.

References: CVE-2008-0706

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Compaq Presario C700 Notebook, HP G7000 Notebook and Compaq Presario A900 Notebook using BIOS versions F.26 and earlier

BACKGROUND

CVSS 2.0 Base Metrics

Reference Base Vector Base Score

CVE-2008-0706 (AV:L/AC:L/Au:N/C:C/I:C/A:C) 7.2

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

Note: This vulnerability only affects customers who use power–on password. However, HP strongly recommends that all customers update to the latest System BIOS version.

RESOLUTION

HP has provided BIOS F.31 or later to resolve this vulnerability. BIOS F.31 is available in SoftPaq SP38646.

To install the latest version of the BIOS, follow the instructions below. Printing the instructions prior to the installation is recommended.

1. Open a web browser and visit <http://www.hp.com>
2. Click on the link for HP Software & Drivers downloads web site
3. On the Support & Drivers page, type the model number in the Search field and then press Enter.
4. Select the operating system currently installed on the notebook.
5. In the BIOS section, click WinFlash for HP Notebook System BIOS. The version should be listed as BIOS F.31 or a later version.
6. Click the Download only button on the page to begin the download of the BIOS update. Save the file to a convenient folder on the PC.
7. Double–click the downloaded file to start the installation. Follow all prompts and restart the notebook when requested by the installation. Do not turn off the notebook until prompted to do so.

Note: It is recommended that the notebook PC use an AC adapter and be connected to the Internet with an Ethernet cable because interruptions in power or wireless connections may result in the download failing to install.

PRODUCT SPECIFIC INFORMATION

None

HISTORY

Version: 1 (rev.1) – 27 March 2008 Initial release

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@xxxxxx

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@xxxxxx

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_driv

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

X = 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/AwUBR+vDqOAFovwtKn1ZEQKGIQCgjXO2VEOVij5SN+HWVCLvTWTtoQsAnRDR
HhdYRRhg0tDxL4mHgd5p4qcB
=6k3N

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