

HPSBUX02324 SSRT080034 rev.1 – HP–UX Running Netscape Directory Server (NDS), Local Gain Extended Privileges

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-05/msg00064.html>

- *From:* security-alert@xxxxxx
 - *Date:* Tue, 06 May 2008 07:13:31 -0700
-

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

Hash: SHA1

SUPPORT COMMUNICATION – SECURITY BULLETIN

Document ID: c01433676

Version: 1

HPSBUX02324 SSRT080034 rev.1 – HP–UX Running Netscape Directory Server (NDS), Local Gain Extended Privileges

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

Release Date: 2008-05-05

Last Updated: 2008-05-05

Potential Security Impact: Local gain extended privileges.

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

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP–UX running Netscape Directory Server (NDS). The vulnerability could be used locally to gain extended privileges.

References: CVE-2008-0892

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP–UX B.11.11, B.11.23, and B.11.31 running Netscape Directory Server (NDS) vB.06.21.40 or earlier and vB.07.10.40 or earlier.

BACKGROUND

CVSS 2.0 Base Metrics

=====

Reference Base Vector Base Score

CVE-2008-0892 (AV:A/AC:L/Au:S/C:C/I:C/A:C) 7.7

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

Netscape Directory Server B.06.21.60 for HP–UX is a release of Netscape’s Directory Server 6.21 from HP.
Netscape Directory Server B.07.10.40 for HP–UX is a release of Netscape’s Directory Server 7.1 from HP.

RESOLUTION

HP has provided the following software updates to resolve this vulnerability.

HP_UX Release
NDS Version

B.11.11, B.11.23, B.11.31
Netscape Directory Server vB07.10.40

B.11.11, B.11.23, B.11.31
Netscape Directory Server vB06.21.60

The updates are available for download from:
<http://www.hp.com/go/softwaredepot/>

MANUAL ACTIONS: Yes – Update
Install Netscape Directory Server vB.06.21.60 or subsequent
Install Netscape Directory Server vB.07.10.40 or subsequent

PRODUCT SPECIFIC INFORMATION

HP–UX Software Assistant: HP–UX Software Assistant is an enhanced application that replaces HP–UX Security Patch Check. It analyzes all Security Bulletins issued by HP and lists recommended actions that may apply to a specific HP–UX system. It can also download patches and create a depot automatically. For more information see: <https://www.hp.com/go/swa>

The following text is for use by the HP–UX Software Assistant.

AFFECTED VERSIONS

HP–UX B.11.11
HP–UX B.11.23
HP–UX B.11.31

=====
NetscapeDirSvr7.NDS–ADM
NetscapeDirSvr7.NDS–BASE
NetscapeDirSvr7.NDS–BSCLNT
NetscapeDirSvr7.NDS–BSJRE
NetscapeDirSvr7.NDS–NC
NetscapeDirSvr7.NDS–NSPERL
NetscapeDirSvr7.NDS–PERLDAP
NetscapeDirSvr7.NDS–RUN
NetscapeDirSvr7.NDS–SLAPD

NetscapeDirSvr7.NDS–SLCLNT
NetscapeDirSvr7.NDS–SVCORE
action: install revision B.07.10.40 or subsequent

NetscapeDirSvr6.NDS–ADM
NetscapeDirSvr6.NDS–BASE
NetscapeDirSvr6.NDS–BSCLNT
NetscapeDirSvr6.NDS–BSJRE
NetscapeDirSvr6.NDS–NC
NetscapeDirSvr6.NDS–NSPERL
NetscapeDirSvr6.NDS–PERLDAP
NetscapeDirSvr6.NDS–RUN
NetscapeDirSvr6.NDS–SLAPD
NetscapeDirSvr6.NDS–SLCLNT
NetscapeDirSvr6.NDS–SVCORE
action: install revision B.06.21.60 or subsequent

END AFFECTED VERSIONS

HISTORY

Version:1 (rev.1) – 05 May 2008 Initial release

Third Party Security Patches: Third party security patches which 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@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_driverAlertProfile

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/AwUBSCBUi+AfOvwtKn1ZEQLonQCfSPVcz7kwW/N7dqT5dsZe8x+nVb8AoIeP
tqBpPluCtzCt0/Rkl6hxEkvk

=PMA1

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