-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

IBM SECURITY ADVISORY

First Issued: Tue Jun 17 04:07:12 CDT 2014

The most recent version of this document is available here:

http://aix.software.ibm.com/aix/efixes/security/openssh_advisory4.asc
https://aix.software.ibm.com/aix/efixes/security/openssh_advisory4.asc
ftp://aix.software.ibm.com/aix/efixes/security/openssh_advisory4.asc
==========
VULNERABILITY SUMMARY

VULNERABILITY: AIX OpenSSH Vulnerability

PLATFORMS: AIX 5.3, 6.1 and 7.1
VIOS VIOS 2.2.*

SOLUTION: Apply the fix as described below.

THREAT: See below

CVE Numbers: CVE-2014-2532,CVE-2014-2653

Reboot required? NO
Workarounds? NO
Protected by FPM? NO
Protected by SED? NO
==========
DETAILED INFORMATION

I. DESCRIPTION

CVE-2014-2532
OpenSSH could allow a remote attacker to bypass security restrictions, caused by the inclusion of wildcard characters in the AcceptEnv lines of the sshd_config configuration file within the sshd program.By using a substring before a wildcard character, an attacker could exploit this vulnerability to bypass intended environment restrictions.

CVE-2014-2653
OpenSSH could allow a remote attacker to bypass security restrictions, caused by an error in the SSH client when handling a HostCertificate. By persuading a victim to visit a specially-crafted Web site containing a malicious certificate, an attacker could exploit this vulnerability using a malicious server to disable SSHFP-checking.

II. CVSS

CVE-2014-2532
CVSS Base Score:5
CVSS Temporal Score:see http://xforce.iss.net/xforce/xfdb/91986
CVSS Environmental Score*:Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:N/A:N)

CVE-2014-2653
CVSS Base Score:4.3
CVSS Temporal Score:see http://xforce.iss.net/xforce/xfdb/92116
CVSS Environmental Score*:Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:N/A:N)

III. PLATFORM VULNERABILITY ASSESSMENT

To determine if your system is vulnerable, execute the following command:

lslpp -L openssh.base

The following fileset levels are vulnerable:

AIX Fileset	Lower Level	Upper Level	KEY
openssh.base	4.0.0.5200	6.0.0.6106	key_w_fs

IV. SOLUTIONS

A fix is available, and it can be downloaded from:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixbp

To extract the fixes from the tar file:

zcat OpenSSH_6.0.0.6107.tar.Z | tar xvf -

IMPORTANT: If possible, it is recommended that a mksysb backup
of the system be created. Verify it is both bootable and
readable before proceeding.

To preview the fix installation:

installp -apYd . OpenSSH_6.0.0.6107

To install the fix package:

installp -aXYd . OpenSSH_6.0.0.6107

V. WORKAROUNDS

No workarounds.

VI. CONTACT INFORMATION

If you would like to receive AIX Security Advisories via email,
please visit:

http://www.ibm.com/systems/support

and click on the "My notifications" link.

To view previously issued advisories, please visit:

http://www14.software.ibm.com/webapp/set2/subscriptions/onvdq

Comments regarding the content of this announcement can be
directed to:

security-alert@austin.ibm.com

To obtain the PGP public key that can be used to communicate
securely with the AIX Security Team you can either:

A. Send an email with "get key" in the subject line to:

security-alert@austin.ibm.com

B. Download the key from our web page:

http://www.ibm.com/systems/resources/systems_p_os_aix_security_pgpkey.txt

C. Download the key from a PGP Public Key Server. The key ID is:

0x28BFAA12

Please contact your local IBM AIX support center for any
assistance.

VII. REFERENCES:

Note: Keywords labeled as KEY in this document are used for parsing purposes.

eServer is a trademark of International Business Machines
Corporation. IBM, AIX and pSeries are registered trademarks of
International Business Machines Corporation. All other trademarks
are property of their respective holders.

Complete CVSS Guide: http://www.first.org/cvss/cvss-guide.html
On-line Calculator V2: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
X-Force Vulnerability Database:http://xforce.iss.net/xforce/xfdb/91986
X-Force Vulnerability Database:http://xforce.iss.net/xforce/xfdb/92116
CVE-2014-2532 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2532
CVE-2014-2653 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2653

*The CVSS Environment Score is customer environment specific and will
ultimately impact the Overall CVSS Score. Customers can evaluate the
impact of this vulnerability in their environments by accessing the links
in the Reference section of this Flash.

Note: According to the Forum of Incident Response and Security Teams
(FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry
open standard designed to convey vulnerability severity and help to
determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES
"AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE
RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY
VULNERABILITY.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.13 (AIX)

iEYEARECAAYFAlOgBk0ACgkQ4fmd+Ci/qhJETQCfVtq+DWv7gvFLrJDdCOgZhJW3
Z2gAn3vdkfKXhola0XTLSez3KigEU8DQ
=SS/P
-----END PGP SIGNATURE-----