

IBM SECURITY ADVISORY

First Issued: Fri Aug 7 15:15:59 CDT 2015
|Updated: Tue Aug 18 09:19:51 CDT 2015
|Update: Added AIX 5.3 vulnerability information

The most recent version of this document is available here:

http://aix.software.ibm.com/aix/efixes/security/sendmail\_advisory2.asc
https://aix.software.ibm.com/aix/efixes/security/sendmail\_advisory2.asc
ftp://aix.software.ibm.com/aix/efixes/security/sendmail\_advisory2.asc

Security Bulletin: Vulnerability in Diffie-Hellman ciphers affects
sendmail on AIX (CVE-2015-4000)

SUMMARY:

The Logjam Attack on TLS connections using the Diffie-Hellman (DH) key
exchange protocol affects sendmail when using the sendmail\_ssl binary on
AIX.

VULNERABILITY DETAILS:

CVEID: CVE-2015-4000
DESCRIPTION: The TLS protocol could allow a remote attacker to obtain
sensitive information, caused by the failure to properly convey a
DHE\_EXPORT ciphersuite choice. An attacker could exploit this
vulnerability using man-in-the-middle techniques to force a downgrade
to 512-bit export-grade cipher. Successful exploitation could allow
an attacker to recover the session key as well as modify the contents
of the traffic. This vulnerability is commonly referred to as
"Logjam".
CVSS Base Score: 4.3
CVSS Temporal Score: See
https://exchange.xforce.ibmcloud.com/vulnerabilities/103294 for the
current score
CVSS Environmental Score\*: Undefined
CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:N)

AFFECTED PRODUCTS AND VERSIONS:

AIX 5.3, 6.1, 7.1
VIOS 2.2.x

The following AIX fileset levels are vulnerable:

Table with 4 columns: AIX Fileset, Lower Level, Upper Level, KEY. Rows include bos.net.tcp.client with various version ranges and key\_w\_fs as the key.

AIX Fileset (VIOS) Lower Level Upper Level

```
-----
bos.net.tcp.client 6.1.0.0(2.2.0.0)    6.1.8.19(2.2.2.6)
bos.net.tcp.client 6.1.0.0(2.2.0.0)    6.1.9.45(2.2.3.50)
```

Note: to find out whether the affected filesets are installed on your systems, refer to the `lslpp` command found in AIX user's guide.

Example: `lslpp -L | grep -i bos.net.tcp.client`

## REMEDIATION:

### A. APARS

IBM has assigned the following APARs to this problem:

Please note that these only apply to the SSL-enabled sendmail binary, `/usr/sbin/sendmail_ssl`. The default sendmail bindary, `/usr/sbin/sendmail`, is not vulnerable to the Logjam attack.

AIX Level	APAR	Availability	SP	KEY
5.3.12	IV75967	N/A	N/A	key_w_apar
6.1.8	IV75644	N/A	N/A	key_w_apar
6.1.9	IV75643	12/04/15	SP6	key_w_apar
7.1.2	IV75645	N/A	N/A	key_w_apar
7.1.3	IV75646	2/26/16	SP6	key_w_apar

Subscribe to the APARs here:

<http://www.ibm.com/support/docview.wss?uid=isglIV75643>  
<http://www.ibm.com/support/docview.wss?uid=isglIV75646>

By subscribing, you will receive periodic email alerting you to the status of the APAR, and a link to download the fix once it becomes available.

### B. FIXES

Fixes are available. Please note that the `sendmail_ssl` fixes require a current version of OpenSSL that includes the Logjam fix. Please see the previously published OpenSSL bulletin:

[http://aix.software.ibm.com/aix/efixes/security/openssl\\_advisory14.asc](http://aix.software.ibm.com/aix/efixes/security/openssl_advisory14.asc)  
[https://aix.software.ibm.com/aix/efixes/security/openssl\\_advisory14.asc](https://aix.software.ibm.com/aix/efixes/security/openssl_advisory14.asc)  
[ftp://aix.software.ibm.com/aix/efixes/security/openssl\\_advisory14.asc](ftp://aix.software.ibm.com/aix/efixes/security/openssl_advisory14.asc)

The `sendmail_ssl` fixes can be downloaded via ftp or http from:

[ftp://aix.software.ibm.com/aix/efixes/security/sendmail\\_fix2.tar](ftp://aix.software.ibm.com/aix/efixes/security/sendmail_fix2.tar)  
[http://aix.software.ibm.com/aix/efixes/security/sendmail\\_fix2.tar](http://aix.software.ibm.com/aix/efixes/security/sendmail_fix2.tar)  
[https://aix.software.ibm.com/aix/efixes/security/sendmail\\_fix2.tar](https://aix.software.ibm.com/aix/efixes/security/sendmail_fix2.tar)

The link above is to a tar file containing this signed advisory, fix packages, and OpenSSL signatures for each package. The fixes below include prerequisite checking. This will enforce the correct mapping between the fixes and AIX Technology Levels.

Please note that these only apply to the SSL-enabled sendmail binary, `/usr/sbin/sendmail_ssl`. The default sendmail bindary, `/usr/sbin/sendmail`, is not vulnerable to the Logjam attack.

AIX Level	Interim Fix (*.Z)	KEY
5.3.12.9	IV75967m9a.150817.epkg.Z	key_w_fix
6.1.8.6	IV75644m6a.150731.epkg.Z	key_w_fix
6.1.9.5	IV75643m5a.150731.epkg.Z	key_w_fix
7.1.2.6	IV75645m6a.150731.epkg.Z	key_w_fix
7.1.3.5	IV75646m5a.150731.epkg.Z	key_w_fix

To extract the fixes from the tar file:

```
tar xvf sendmail_fix2.tar
cd sendmail_fix2
```

Verify you have retrieved the fixes intact:

The checksums below were generated using the "openssl dgst -sha256 file" command as the following:

KEY	openssl dgst -sha256	filename
-----	-----	-----
	9fc6906b826799ee6e98b1da7e4a7f3b41d8db515be46ee043565e6440487015	
IV75967m9a.150817.epkg.Z	key_w_csum	
	517637a4871e869ea9322d8c91c94ef8c74ee17821fbdf85f84e52dfd99233f8	
IV75644m6a.150731.epkg.Z	key_w_csum	
	af34ca8e20e0440a35dd4fd8caaa051b892f4d30f7cb7fa3f179efcd7f7ab834	
IV75643m5a.150731.epkg.Z	key_w_csum	
	e8916a64220b50eb24df48276fb2a8ddb50e7c42286eee52841aa7e14864c7c	
IV75645m6a.150731.epkg.Z	key_w_csum	
	ea4f46484d3934fd9df73293f0ca47abcb38f930e8e5f619fa2af720e390dc4d	
IV75646m5a.150731.epkg.Z	key_w_csum	

These sums should match exactly. The OpenSSL signatures in the tar file and on this advisory can also be used to verify the integrity of the fixes. If the sums or signatures cannot be confirmed, contact IBM AIX Security at [security-alert@austin.ibm.com](mailto:security-alert@austin.ibm.com) and describe the discrepancy.

```
openssl dgst -sha1 -verify <pubkey_file> -signature <advisory_file>.sig
<advisory_file>
```

```
openssl dgst -sha1 -verify <pubkey_file> -signature <ifix_file>.sig <ifix_file>
```

Published advisory OpenSSL signature file location:

```
http://aix.software.ibm.com/aix/efixes/security/sendmail_advisory2.asc.sig
https://aix.software.ibm.com/aix/efixes/security/sendmail_advisory2.asc.sig
ftp://aix.software.ibm.com/aix/efixes/security/sendmail_advisory2.asc.sig
```

### C. FIX AND INTERIM FIX INSTALLATION

**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 a fix installation:

```
installp -a -d fix_name -p all # where fix_name is the name of the
# fix package being previewed.
```

To install a fix package:

```
installp -a -d fix_name -X all # where fix_name is the name of the
```

# fix package being installed.

Interim fixes have had limited functional and regression testing but not the full regression testing that takes place for Service Packs; however, IBM does fully support them.

Interim fix management documentation can be found at:

<http://www14.software.ibm.com/webapp/set2/sas/f/aix.efixmgmt/home.html>

To preview an interim fix installation:

```
emgr -e ipkg_name -p          # where ipkg_name is the name of the
                              # interim fix package being previewed.
```

To install an interim fix package:

```
emgr -e ipkg_name -X          # where ipkg_name is the name of the
                              # interim fix package being installed.
```

You should verify applying this configuration change does not cause any compatibility issues. If you change the default setting after applying the fix, you will expose yourself to the attack described above. IBM recommends that you review your entire environment to identify other areas where you have enabled the Diffie-Hellman key-exchange protocol used in TLS and take appropriate mitigation and remediation actions.

#### WORKAROUNDS AND MITIGATIONS:

None.

---

#### CONTACT US:

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

<http://www.ibm.com/support/mynotifications>

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](mailto:security-alert@austin.ibm.com)

To obtain the OpenSSL public key that can be used to verify the signed advisories and ifixes:

Download the key from our web page:

[http://www.ibm.com/systems/resources/systems\\_p\\_os\\_aix\\_security\\_pubkey.txt](http://www.ibm.com/systems/resources/systems_p_os_aix_security_pubkey.txt)

To obtain the PGP public key that can be used to communicate securely with the AIX Security Team via [security-alert@austin.ibm.com](mailto:security-alert@austin.ibm.com) you can either:

A. Download the key from our web page:

[http://www.ibm.com/systems/resources/systems\\_p\\_os\\_aix\\_security\\_pgppubkey.txt](http://www.ibm.com/systems/resources/systems_p_os_aix_security_pgppubkey.txt)

B. 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.

REFERENCES:

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>

ACKNOWLEDGEMENTS:

CVE-2015-4000 was reported to IBM by The WeakDH team at <https://weakdh.org>

CHANGE HISTORY:

First Issued: Fri Aug 7 15:15:59 CDT 2015  
Updated: Tue Aug 11 09:47:52 CDT 2015  
Update: Changed advisory name to sendmail\_advisory2.asc and fix pack to  
sendmail\_fix2.tar  
| Updated: Tue Aug 18 09:19:51 CDT 2015  
| Update: Added AIX 5.3 vulnerability information

=====  
\*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 Security Bulletin.

Disclaimer

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.