Hewlett Packard Enterprise

HPE Software Security Update

HPE Propel Update for "Bar Mitzvah" Vulnerability (CVE-2015-2808)

Document management:

Date	Version	Change
3-Oct-2016	1.0	Initial Release

Summary:

From https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2808:

> The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.

Topic

Find out more about CVE-2015-2808 from the **MITRE CVE dictionary**.

HPE has investigated the CVE-2015-2808 vulnerability in relation to HPE Propel. This document provides required actions that must be performed to mitigate this vulnerability.

Affected Releases: 1.01, 1.11, 2.01, 2.10, 2.20

ACTION: Review all details in instructions provided in this paper to address the vulnerability.
HPE SW recommend to address this information as soon as possible.

Response

Impact on HPE Propel

The 1.01, 1.11, and 2.01 versions of the HPE Propel OVA (Virtual Appliance) ship with older versions of Node.js which are vulnerable to CVE-2015-2808. Additionally, versions 1.01 and 1.11 require updates to JBoss to disable use of the RC4 cipher. Finally, all versions need to reconfigure HPE Operations Orchestration to remove the RC4 cipher.

Mitigation Actions

For v2.01:

```
# yum -y remove nodejs
```

For v1.0, v1.11 and v2.01, update Node.js to the latest stable release:

```
# curl -sL https://rpm.nodesource.com/setup_4.x | bash -
# yum -y --disablerepo "*" --enablerepo "nodesource" install nodejs
```

After mitigation, ‘node –v’ should report v4.4.6 or newer.

For 2.X, edit:

```
/etc/httpd/conf.d/ssl.conf
```

to exclude RC4 by appending “**!RC4**” (without quotes) to the SSLCipherSuite configraution:

```
SSLCipherSuite [existing configuration]:!RC4
```

For v1.X, update:

```
/opt/hp/propel/jboss-as/standalone/configuration/standalone.xml
```

to use the following cipher suite in the HTTPS connector:

```
<connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https"
secure="true">
```

```
        <ssl name="ssl" key-alias="<myhost.mycompany.com>" password="<password>"
certificate-key-file="/opt/hp/propel/security/.keystore" cipher-
suite="TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA" protocol="TLSv1" verify-
client="false"/>
    </connector>
```

For all versions, update:

```
/opt/hp/oo/central/tomcat/conf/server.xml
```

to use the following ciphers:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" clientAuth="false"
compression="on" keyAlias="tomcat" keyPass="changeit"
keystoreFile="/opt/hp/oo/central/var/security/key.store"
keystorePass="changeit" keystoreType="JKS" maxThreads="200" port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
secure="true" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLSv1.2"
truststoreFile="/opt/hp/oo/central/var/security/client.truststore"
truststorePass="changeit" truststoreType="JKS"
ciphers="TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256"/>
```

After updating Node.js and modifying Apache, JBoss and OO configurations as appropriate for your HPE Propel version, restart all services:

For 2.X:

```
# service httpd restart
```

For all versions:

```
# service central restart
# propel stop
# propel start
```