PCI Compliance and Software Versions

Overview

Most PCI compliance scanning systems use a specific software package version number that contains a reported vulnerability. This document discusses some of the specific software packages that contain known vulnerabilities. This document will also help you determine whether developers used the backport process to patch a software package.

What is backporting?

The backport process allows the operating system vendor to change only the parts of the software that the security vulnerability affected. In this way, it avoids the introduction of new features that the developers did not test. This process does not increment the version number. Instead, the developers attach a flag to the package.

Operating system developers often backport updates to avoid the need to distribute a new version of the software package.

For example, an operating system developer may combine OpenSSL 0.9.7c with a patch from OpenSSL 0.9.7.d to create OpenSSL 0.9.7c-2. If most PCI scanning systems look for OpenSSL version 0.9.7d or higher, they may incorrectly show OpenSSL 0.9.7c-2 as vulnerable. In this case, you would inform the PCI compliance company that you use a backported version of the software package, which its developers patched for the vulnerability. Your PCI compliance company can then record your software version and mark a false positive in the scan results.

OpenSSL

Many different system services and packages use OpenSSL. To check your OpenSSL installation for backporting, perform the following steps:

1. Determine which OpenSSL package exists on your system. To do this, run the following command:

   ```
   rpm -qa | grep openssl
   ```

   The following example output indicates that your server runs version `openssl-0.9.8e-36` of OpenSSL:

   ```
   openssl-0.9.8e-36.el5_11
   openssl-0.9.8e-36.el5_11
   ```

2. To check the RPM change log for vulnerability fixes that the version includes, run the following command:

   ```
   rpm --changelog -q openssl-0.9.8b-10.el5 | less
   ```

3. The RPM change log may include fixes for the CVEs that your PCI compliance scanning company requires. If these fixes appear, inform

them of the patched version and which CVEs it includes so that they can mark it as a false positive.

SSLCipherSuite

Important:
The SSLCipherSuite directive in the *Global Configuration* section of WHM's *Apache Configuration* interface (*WHM >> Home >> Service Configuration >> Apache Configuration*) defaults to a PCI compliant value as of cPanel & WHM version 66. If your SSLCipherSuite does not pass PCI Compliance scans, open a support ticket.

To adjust your server for PCI compliance, you **must** configure the SSLCipherSuite directive's value in the *Global Configuration* section of WHM's *Apache Configuration* interface (*WHM >> Home >> Service Configuration >> Apache Configuration*). If you set the directive's value and PCI compliance scans of port 443 do not pass, other SSLCipherSuite entries may exist in the `/etc/apache2/conf/ httpd.conf` file. To correct this problem, perform the following steps:

1. Check for additional SSLCipherSuite entries in the `/etc/apache2/conf/ httpd.conf` file. To do this, run the following command:

```
grep -i sslciphersuite /etc/apache2/conf/httpd.conf
```

2. Check your VirtualHosts. To do this, run the following command:

```
grep sslciphersuite /var/cpanel/userdata/*/*_SSL
```

3. If this step returns any results, remove the SSLCipherSuite entries that already exist. To do this, run the following command:

```
perl -pi -e 's{sslciphersuite:.*}{}ms;' path/to/file/from/step/2
```

4. After you remove any SSLCipherSuite entries, rebuild your `httpd.conf` file. To do this, run the following command:

```
/usr/local/cpanel/scripts/rebuildhttpdconf
```

5. Confirm that only one global SSLCipherSuite entry exists. To do this, run the following command:

```
grep -i sslciphersuite /etc/apache2/conf/httpd.conf
```

6. If only one global entry exists, restart Apache. To do this, run the following command:

```
/scripts/restartsrv_httpd
```

7. Rescan port 443 for PCI compliance.

OpenSSH

To determine which OpenSSH package exists on your system, run the following command:

```
rpm -qa | grep openssh
```

The output may resemble the following example:

```
openssh-clients-5.3p1-94.el6.i686
openssh-server-5.3p1-94.el6.i686
openssh-5.3p1-94.el6.i686
```

This output indicates that `openssh-5.3pl-94.e16` exists as your OpenSSH version. This OpenSSH version may result in a PCI scan that returns the following two vulnerabilities:

- OpenSSH J-PAKE Session Key Retrieval Vulnerability — This issue does **not** affect OpenSSH as shipped with RedHat Enterprise Linux® (RHEL) versions 6 and 7. For more information, read CVE-2010-4478 on RedHat's web site.
- OpenSSH "`child_set_env()`" Security Bypass Issue —This issue minimally impacts security and does **not** pose a severe risk to most systems. Even though this OpenSSH version 6.6 addressed this issue, the RHEL repositories do **not** contain this updated version. If you wish to update OpenSSH to the new version, you **must** install it manually.

If the OpenSSH package `6.6.1p1-35.el7_3` exists on your server, your output will resemble the following example:

```
openssh-6.6.1p1-35.el7_3.x86_64
openssh-server-6.6.1p1-35.el7_3.x86_64
openssh-clients-6.6.1p1-35.el7_3.x86_64
```

This OpenSSH package contains a vulnerability that affects the way it handles authentication by users who do not exist on the system. To mitigate this issue, enable the Security-Enhanced Linux (SELinux) security module that ships with RHEL versions 6 and 7.

For more information about this vulnerability, read CVE-2016-6210 on RedHat's Website.

Exim

cPanel & WHM includes patches that help to make Exim PCI compliant. The RPM change log includes information about these patches.

Simple Mail Transfer Protocol

PCI Compliance requires email client encryption. Your email client provides SSL and TLS encryption. To confirm your server's SMTP transactions remain encrypted, perform the following steps as the `root` user:

1. Navigate to the *Exim Configuration Manager* interface (*WHM >> Home >> Service Configuration >> Exim Configuration Manager*).
2. Enable the *Require clients to connect with SSL or issue the STARTTLS command before they are allowed to authenticate with the server* . option.

   > **Note:**
   > As of cPanel & WHM version 66, this option defaults to *Enabled*.

3. Click *Save*.

Backported CVEs

To view the CVE-related fixes in your version of Exim, run the following command:

```
rpm -q --changelog exim | grep CVE
```

The output will display the CVE number, for example:

```
fix for CVEs CVE-2010-2024, CVE-2010-2023
Update CVE-2011-0017 patch to fix use of -C flag by unprivileged users.
CVE-2011-0017: Backport patch from EXIM 4.74 for arbitrary file overwrite
bug.
CVE-2010-4344: Apply string_format buffer overflow patch
CVE-2010-4345: Compile with ALT_CONFIG_PREFIX=/etc/exim
CVE-2010-4345: Compile with ALT_CONFIG_PREFIX=/etc
```

To report the CVE fixes that your Exim installation includes, send the output that reflects the patched software to your PCI scanning company.

TLS

PCI compliance requires that your server run TLS version 1.2 or greater. For more information, read the Security Standards Council's® Date Change for Migrating from SSL and Early TLS article and our cPanel Deprecation Plan documentation.

FTP

We **strongly** recommend that you disable FTP services and use SFTP, SCP, or WebDisk for file transfers.

If you cannot disable FTP services, we recommend that you use WHM's *FTP Server Selection* interface *(WHM >> Home >> Service Configuration >> FTP Server Selection)* to configure your server to use ProFTPd.

Then, use WHM's *FTP Server Configuration* interface *(WHM >> Home >> Service Configuration >> FTP Server Configuration)* to configure ProFTPd to use TLS v1.2

TLS

PCI compliance requires that your server run TLS version 1.2 or greater. For more information, read the Security Standards Council's® Date Change for Migrating from SSL and Early TLS article and our cPanel Deprecation Plan documentation.

Bind

Although cPanel & WHM does not create BIND, all cPanel & WHM servers servers include BIND by default. Vendor updates will typically resolve PCI compliance issues.

BIND CVE-2011-4313

The BIND change log does not show `CVE-2011-4313` directly. Instead, the change log shows under `RHEL #754398`.

Run the following command to test for the presence of this fix:

```
rpm -q --changelog bind | grep 754398
```

Your output should resemble the following example:

```
- fix DOS against recursive servers (#754398)
```

To report the CVE fixes that your BIND installation includes, send the output that reflects the patched software to the PCI scanning company.

Hide the BIND Version

To become PCI compliant, you **must** hide the BIND version on your server.

To do this, perform the following steps:

1. Connect to the server via SSH as the `root` user.
2. Edit `the /etc/named.conf` file and add the following line of code to the `options` section:

```
version "";
```

3. Use the following command to restart BIND:

```
/usr/local/cpanel/scripts/restartsrv_named
```

4. Rescan your server with your account on the PCI company's website.

Hide the DNS Server Hostname

To become PCI compliant, you **must** hide your DNS server's hostname.

To do this, perform the following steps:

1. Connect to the server via SSH as the `root` user.
2. Edit `/etc/named.conf` and add the following line of code to the `options` section:

```
hostname "";
```

3. Use the following command to restart BIND:

```
/scripts/restartsrv_named
```

4. Rescan your server with your account on the PCI company's website.

Mailman

You can completely disable Mailman when you scan for PCI Compliance.

To disable Mailman, perform the following steps:

1. Log in to WHM as the `root` user.
2. In the *Mail* section of the *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings*), set the *Enable Mailman mailing lists* setting to *Off.*
3. Click *Save*.

If you do not want to disable Mailman, perform the following steps to pass a PCI Compliance scan:

1. Log in to to the server as the `root` user via SSH.
2. Create the following file to deny web requests for Mailman:

```
/usr/local/cpanel/3rdparty/mailman/cgi-bin/.htaccess
```

The contents of the file should appear similar to the following example:

```
<Limit GET POST>
 order deny, allow
 <deny from all>
 </Limit>

<Limit PUT DELETE>
 order deny, allow
 <deny from all>
 </Limit>
```

3. Rescan your server with your account on the PCI company's website.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- PCI Compliance and Software Versions
- How to Adjust Cipher Protocols
- How to Prevent Spam with Mail Limiting Features
- How to Configure the Exim Outgoing IP Address
- CVE-2017-1000369 Exim - Stack Clash

- How to Create Mail Filter Rules For Mailing Lists
- How to Migrate the Contents of Email Accounts in Addon Domains
- How to Use cPanel API Tokens
- Security
- Man-in-the-Middle Attacks

- PCI Compliance and Software Versions
- How to Adjust Cipher Protocols
- How to Prevent Spam with Mail Limiting Features
- How to Configure the Exim Outgoing IP Address
- CVE-2017-1000369 Exim - Stack Clash

- UAPI Functions - Email::delete_list
- UAPI Functions - Email::list_lists
- cPanel API 2 Functions - Email::set_archiving_default_configuration
- cPanel API 2 Functions - Email::get_archiving_types
- cPanel API 2 Functions - Email::listlists