CVE-2016-1238 Perl

Background Information

On July 25 2016, Perl announced a vulnerability in all versions of the Perl 5 software.

Impact

According to Perl development:

> *The problem relates to Perl 5 ("perl") loading modules from the includes directory array ("@INC") in which the last element is the current directory ("."). That means that, when "perl" wants to load a module (during first compilation or during lazy loading of a module in run-time), perl will look for the module in the current directory at the end, since '.' is the last include directory in its array of include directories to seek. The issue is with requiring libraries that are in "." but are not otherwise installed.*

Under some conditions, e.g. changing the current directory to a location writable by other users, this vulnerability can lead to arbitrary code execution.

Releases

cPanel & WHM version 56 and greater are already protected. Versions previous to 56 received updates to mitigate this issue as of TSR-2016-0002 for cPanel-provided scripts. Versions greater than the versions listed below are protected:

11.50 - 11.50.5.0
11.52 - 11.52.4.0
11.54 - 11.54.0.18

For more information about the protections already in place, read our 56 Release Notes.

Additional updates have been published to protect upstream-provided Perl 5 scripts shipped in the cPanel-provided Perl distribution for versions previous to 56. Versions greater than the versions listed below include the additional protections for upstream-provided scripts:

11.52 - 11.52.6.4
11.54 - 11.54.0.27

How to determine if your server is up-to-date

For versions 56 and greater, the previously updated RPMs provided by cPanel will contain a changelog entry noting the applied fixes. You can check for the changelog entry in versions 56 and greater with the following command:

```
rpm -q --changelog cpanel-perl-522 | grep "Remove . from @INC"
```

The output should resemble below:

```
- Remove . from @INC unless the environment variable PERL_USE_UNSAFE_INC=1 is set.
```

For versions 54 and 52, the updated RPMs provided by cPanel will contain a changelog entry with the CVE number. You can check for the changelog entry in versions 54 and 52 with the following command:

```
rpm -q --changelog cpanel-perl-514 | grep CVE-2016-1238
```

The output should resemble below:

```
- Fix for CVE-2016-1238
```

What to do if you are not up-to-date

If your server is not running one of the above versions, update immediately.

To upgrade your server, navigate to WHM's *Upgrade to Latest Version* interface (*WHM >> Home >> cPanel >> Upgrade to Latest Version*) and click *Click to Upgrade*.

To upgrade cPanel from the command line, run the following commands:

```
/scripts/upcp
/scripts/check_cpanel_rpms --fix --long-list
```

For versions 56 and greater, verify the updated Perl RPM was installed:

```
rpm -q --changelog cpanel-perl-522 | grep "Remove . from @INC"
```

The output should resemble below:

```
- Remove . from @INC unless the environment variable PERL_USE_UNSAFE_INC=1 is set.
```

For versions 54 and 52, verify the updated Perl RPM was installed:

```
rpm -q --changelog cpanel-perl-514 | grep CVE-2016-1238
```

The output should resemble below:

```
- Fix for CVE-2016-1238
```

Credit: This issue was discovered and reported by J.D. Lightsey and Todd Rinaldo, courtesy of the cPanel Security Team.
CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1238

Additional documentation

- CVE-2016-1238 Perl
- How to Update Your System
- Troubleshooting Guide for Perl and CGI Scripts
- How to Configure Your Firewall for cPanel Services
- How to purchase CloudLinux