CVE-2016-1531 Exim

RELEASED TO PUBLIC

Background Information

On Wednesday, March 2, 2016, Exim announced a vulnerability in all versions of the Exim software.

Impact

According to Exim development: "*All installations having Exim set-uid root and using 'perl_startup' are vulnerable to a local privilege escalation. Any user who can start an instance of Exim (this is normally *any* user) can gain root privileges.*"

Releases

The following versions of cPanel & WHM were patched to have the correct version of Exim. All previous versions of cPanel & WHM, including 11.48.x and below, are vulnerable to a set-uid attack on Exim.

TIER	VERSION
11.50	11.50.5.0
11.52	11.52.4.0
11.54	11.54.0.18
EDGE	11.55.9999.106
CURRENT	11.54.0.18
RELEASE	11.54.0.18
STABLE	11.54.0.18

How to determine if your server is up to date

The updated RPMs provided by cPanel will contain a changelog entry with the CVE number. You can check for this changelog entry with the following command:

```
rpm -q --changelog exim | grep CVE-2016-1531
```

The output should resemble below:

```
- Fixes CVE-2016-1531
```

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, use WHM's *CVE-2016-1531 Exim* interface (*WHM >> Home >> cPanel >> Upgrade to Latest Version).*

Alternatively, you can run the below commands to upgrade your server from the command line:

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

Verify the new Exim RPM was installed:

```
rpm -q --changelog exim | grep CVE-2016-1531
```

The output should resemble below:

```
- Fixes CVE-2016-1531
```

What has changed?

Exim now provides two configuration options which limit what environment variables are available to Exim and all of its child processes. The variables are **keep_environment** and **add_environment**. For the initial release with this feature, cPanel will be setting the variables as follows in all supported cPanel & WHM systems. These values can be modified in the Advanced Configuration Editor if necessary, though we advise caution on adding too many variables to keep_environment.

/etc/exim.conf

```
keep_environment = X-SOURCE : X-SOURCE-ARGS : X-SOURCE-DIR
add_environment =
PATH=/usr/local/sbin::/usr/local/bin::/sbin::/bin::/usr/sbin::/usr/bin::
/sbin::/bin
```

If you are still experiencing issues or need additional help, please contact cPanel support.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- How to Configure the Exim Outgoing IP Address
- CVE-2017-1000369 Exim - Stack Clash
- CVE-2016-9963 Exim
- How to Customize the Exim System Filter File
- Scan Outgoing Mail

Error rendering macro 'contentbylabel' : parameters should not be empty

- How to Configure the Exim Outgoing IP Address
- CVE-2017-1000369 Exim - Stack Clash
- CVE-2016-9963 Exim
- How to Customize the Exim System Filter File
- Scan Outgoing Mail

- WHM API 1 Functions - get_unique_sender_recipient_count_per_user
- WHM API 1 Functions - get_unique_recipient_count_per_sender_for_user
- WHM API 1 Functions - validate_exim_configuration_syntax
- WHM API 1 Sections - Mail
- WHM API 1 Functions - get_mailbox_status