CVE-2017-1000369 Exim - Stack Clash

RESOLVED

Background Information

On Monday, June 19, 2017, Qualsys announced memory handling vulnerabilities in a number of software distributions, including a vulnerability that could leverage a bug in the Exim software to achieve a local privilege escalation to root.

Impact

Vulnerable versions of Exim can be susceptible to local privilege escalation to root.

Releases

TIER	VERSION
64	64.0.30
62	62.0.25
CURRENT	64.0.30
RELEASE	64.0.30
STABLE	64.0.30

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-2017-1000369
```

The output should resemble below:

```
- Applied patch for CVE-2017-1000369
```

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 *Upgrade to Latest Version* 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-2017-1000369
```

The output should resemble below:

```
- Applied patch for CVE-2017-1000369
```

Additional documentation

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