CVE-2016-9963 Exim

RESOLVED

Background Information

On Sunday, December 25, 2016, Exim announced a vulnerability in versions 4.69 to 4.87 of the Exim software.

Impact

According to Exim development: "If several conditions are met, Exim leaks private information to a remote attacker."

Depending on configuration options for Exim, a domain's DKIM signing keys can be leaked to Exim log files. Additionally, if the EXPERIMENTAL_DSN_INFO=yes build flag is used, DKIM signing keys can be leaked to a remote attacker.

Exim log files are normally not readable by unprivileged users on cPanel & WHM systems. Additionally, cPanel & WHM does not provide an Exim installation with the EXPERIMENTAL_DSN_INFO=yes build flag and does not leak DKIM signing keys to remote attackers based on currently available information. As such, the most severe impacts of CVE-2016-9963 do not apply to cPanel & WHM systems.

Releases

The following versions of cPanel & WHM were patched to have the correct version of Exim.

TIER	VERSION
62	62.0.1
60	60.0.31
58	58.0.41
56	56.0.41
54	54.0.34
EDGE	62.0.1
CURRENT	62.0.1
RELEASE	60.0.31
STABLE	60.0.31

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-2016-9963
```

The output should resemble below:

```
- Patch for CVE-2016-9963
```

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-2016-9963
```

The output should resemble below:

```
    - Patch for CVE-2016-9963
```

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