CVE-2015-0235 GHOST

This article was last updated on: **Apr 09, 2018 14:11**

RESOLVED This article will receive no further updates at this time.

Background Information

On 27 January 2015, a vulnerability in all versions of the GNU C library (glibc) was announced by Qualys. The issue was a buffer overflow during DNS hostname resolution. Disclosure of this issue was coordinated with the various operating system vendors and patches were made available by RedHat soon after the initial announcement went out.

Impact

According to Qualys, this vulnerability allows unauthenticated remote code execution in any daemons or services that perform hostname lookups using the vulnerable functions in the GNU C library. This library is at the core of most services and software that runs on Linux systems.

Qualys developed working attacks for the EXIM mail transport agent that all cPanel & WHM systems use. Qualys also created a Metasploit module to make testing or exploitation of the vulnerability straightforward for an attacker. At present, Qualys has not released any attack code, only detailed analysis of the flaw and its impact.

How to determine if your server is affected

The updated RPMs provided by RedHat, CentOS, and CloudLinux should contain a changelog entry with the CVE number. You can check for this changelog entry with the following command:

```
rpm -q --changelog glibc | grep CVE-2015-0235
```

If a changelog line is displayed, the server has the updated RPMs installed.

Resolution

cPanel does not provide the glibc RPM. It is provided by the vendor of the operating system where cPanel & WHM is installed.

To fix this issue, run the following commands:

```
yum clean all ; yum update glibc
```

Verify the new glibc RPM was installed again:

```
rpm -q --changelog glibc | grep CVE-2015-0235
```

Then reboot the server or manually restart all running services, as RHEL-based systems do not restart running daemons when libc is updated. A reboot or restart of all services is needed.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

Openwall: GHOST CVE-2015-0235

Red Hat: Critical Security Update, Linux 5

Red Hat: Critical Security Update, Linux 6 and 7

CloudLinux: GHOST CVE-2015-0235

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

- Additional Security Software
- CVE-2015-0235 GHOST
- How to Set Up (PHP) Composer
- CVE-2016-3714 ImageMagick
- Third-Party Software End Of Life Policy

- Guide to Third-Party AutoSSL Provider Modules
- WHM API 1 Functions - installed_versions
- WHM API 1 Functions - fetch_security_advice
- WHM API 1 Functions - get_autossl_log
- WHM API 1 Functions - get_autossl_providers