Vulnerabilities

Latest statements from Swivel Secure on the ShellShock, Poodle, GHOST, LogJam, SHA-1 deprecation, Glibc:

Contents

Glibc

Thursday 25th February 2016 12:18 GMT

Version 2.x Appliances are not affected due to the fact that the vulnerability affects versions of glibc 2.9 or higher. V2 Appliances are running version 2.3.4 of glibc.

Version 3 Appliances use libraries that are vulnerable, but we are evaluating the updates, and will be rolling once quality assurance is complete.

CVE-ID:

- CVE-2015-7547

https://access.redhat.com/security/cve/cve-2015-7547

SHA-1 Deprecation

Tuesday 8th December 2015 09:24 GMT

SHA1 is being deprecated by browsers (Internet Explorer, Firefox, Google Chrome etc) and the deadline for its scheduled disappearance is 31/12/2016. Therefore, the trusted certificate authorities will not be issuing certificates expiring after this date.

We can confirm that v2.0.16 and V3 Appliances support SHA2 algorithms. In order to install a new SSL certificate using SHA2, you must follow the guide: How to Install a SSL Certificate

Diffie-Hellman Keys (LogJam)

Wednesday 15th July 2015 09:38 BST

Following the Firefox 39 update which is includes a security enhancement for the LogJam vulnerablity, has blocked web servers that use weak Diffie-Hellman keys.

We recommend that you enforce 128 bit encryption on Tomcat, in order to combat the LogJam vulnerability. Please see: https://kb.swivelsecure.com/wiki/index.php/Ciphers_How_To_Guide

Weak Ciphers:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA

Tuesday 10th February 2015 14:04 GMT

We can confirm that the Swivel Appliances are NOT vulnerable to the GHOST (glibc) vulnerability as the Appliances run on the OS of Red Hat Enterprise Linux 4 (RHEL4).

Please see the following URL to see the list of vulnerable operating systems. You may notice that RHEL4 ELS (Extended Life Cycle Support) is apart of the link. Fortunately, the Swivel Servers do NOT have the ELS associated.

https://access.redhat.com/articles/1332213

Poodle

Tuesday 28th October 2014 15:39

We have developed a new patch which supersedes all previous downloads. This includes previous fixes issued for ShellShock as well fixes to address the new Poodle vulnerabilities:

patch.795.appliance.update.tar.gz

IMPORTANT: Please update your appliance to 2.0.16 prior to installation of this patch.

See Also SSL vulnerability updates stop Mon working and SSL vulnerability updates stop Appliance Synchronisation working

This latest update fixes:

- CVE-2014-6271 (original shellshock);
- CVE-2014-6277 (segfault);
- CVE-2014-6278 (Florian's patch);
- CVE-2014-7169 (taviso bug);
- CVE-2014-7186 (redir_stack bug);
- CVE-2014-7187 (nested loops off by one);
- CVE-2014-//// (exploit 3 on http://shellshocker.net/);
- Poodle SSL vulnerability on standard Tomcat ports (if you have custom ports other than 8080 and 8443, then please install the patch, and compare/check your custom ports in /usr/local/tomcat/conf/server.xml against standard port entries);
- Poodle SSL vulnerability on Webmin;

Shellshock

Wednesday 1st October 2014 09:33

We have developed a new patch which covers the original issue, plus further vulnerabilities (CVE-2014-6271, CVE-2014-7186 and CVE-2014-7187) related to ShellShock. This new patch is available for download and supersedes the previous patch issued below. The process for installing a Swivel Hardware or Virtual appliance patch is given here: Patch Appliance Install, although this patch is available for Swivel versions 2.0.9a onwards.

Monday 29th September 2014 16:41

In response to various questions received, we can confirm that the patches are compatible with appliance versions 2.0.9a onwards, with VMs for both VMware and Hyper-V, and there is no minimum Swivel core requirement. The patch can be applied without the need to stop any essential processes, so authentication is unaffected.

Monday 29th September 2014 16:22

Following the initial disclosure, 3 other vulnerabilities have been discovered: CVE-2014-6271, CVE-2014-7186 and CVE-2014-7187. The patch listed below includes a fix for the first of these, but not the other two. A new patch is in development and will be released shortly.

Friday 26th September 2014 15:33:

An appliance patch is now available for download.

```
Important: When you place the patch into /backups/upload and select the
'Update Appliance/Swivel' option from the 'Advanced Menu', if the option
to 'Remove patch temporary files' appears, you must perform this step
first. This will prevent you from reapplying a previously used patch
which could cause an authentication outage.

Once you have applied the patch, you will notice that you are able to
'Import patch file: patch.515.appliance.update.tar.gz'. After you have
imported the patch, select 'Display Patch information' to read the patch
information and confirm that the patch you are about to Apply is correct.

When you are ready to apply the patch select the 'Apply Patch' option.

The patch will then be applied to the appliance:

Please wait, installing Appliance update.
######################################### [100%]
######################################### [100%]

Update applied, there is no need to reboot the Appliance.
```

Friday 26th September 2014 14:04:

```
"Just to be clear: Swivel software installed upon Windows servers instead
of the Swivel appliance, is not affected by this issue. This only affects
the Swivel appliance which is Linux based."
```

Friday 26th September 2014 12:20:

```
"We hope to have an update the Bash RPM in the form of a Swivel appliance
patch by next week. This will need to undergo some testing prior to
release.

In the meantime, some steps you may take to reduce your exposure are:

* Issue the service webmin stop command on the command line;
* Change the admin user CMI password from the default."
```

Friday 26th September 2014 09:44:

```
?Swivel Secure are aware of a report vulnerability in bash
http://www.cvedetails.com/cve/CVE-2014-6271/ known as ShellShock. This
affects a number of versions of bash, including the version on the
Swivel Appliance

Swivel Secure?s advice is and always has been to restrict appliance
access (port 22 shell and port 10000 for webmin) to internal IP
addresses only. If this precaution is taken, then we believe that there
is no way to exploit this vulnerability on the Swivel Appliance.

Swivel will continue to monitor the situation and monitor the
availability of suitable patches to the underlying appliance OS for this
vulnerability.?
```