SECURITY ADVISORY

#CVE-2014-3513 and CVE-2014-3567 published on Oct. 15th, 2014

Summary Description

On October 15th, 2014, CVE-2014-3513 (https://access.redhat.com/security/cve/CVE-2014-3513) and CVE-2014-3567 (https://access.redhat.com/security/cve/CVE-2014-3567) were published, revealing a couple of memory leak bugs in OpenSSL that could potentially be used for denial of service.

A10 Networks has not been able to replicate this condition, but due to the fact the vulnerable code is included in the software image, A10 Networks will perform an OpenSSL upgrade in combination with the upgrade due to CVE-2014-3566 and support for TLS_FALLBACK_SCSV.

Details

CVE-2014-3513 exposes vulnerability where chunks up to 64k could leak if an attacker sends a specially crafted handshake message. This can be used to exhaust the application's memory, effectively creating a memory leak.

In order for this bug to manifest, it is necessary for OpenSSL to include SRTP code, even though it may not be configured. A10 code base is compiled without support for SRTP, so no devices are affected by this vulnerability.

CVE-2014-3567 exposes a bug where OpenSSL fails to free memory if a session ticket integrity check fails. This can be used for denial of service through memory exhaustion. A10 devices that implement SSL in hardware do not support that option and are thus not vulnerable. All SoftAX and TH930 (when used without SSL accelerator cards) implementations do use OpenSSL that is vulnerable and A10 is working on providing a patch for those.

Vulnerability Assessment

Affected Platforms: *SoftAX, TH930 (when using software SSL)*

Affected Software Versions: 2.7.1-P5, 2.7.2-P3, 2.6.1.-GR1-p13, 2.7.0-p6

Mitigation Recommendations and Patch Information

At this point, a patch is being developed that will also provide support for TLS_FALLBACK_SCSV in response to CVE-2014-3566.

Technology	Major Release	Fixed
HVA	2.7.1-P5	2.7.1-P6
HVA	2.7.2-P3	2.7.2-P4
HVA	2.6.1.-GR1-p13	2.6.1.-GR1-p14
HVA	2.7.0-p6	2.7.0-p7

Work-Around:

As immediate workarounds, A10 customers should update their software and monitor memory consumption of the device.

A10 is researching the possibility of blocking this using aFlex rules.