ip.buffer Security Notifications 2014-10-23

Please see: http://www.scannex.com/appnotes for more security related information.

Heartbleed CVE-2014-0160

Info: OpenSSL can silently bleed information to an attacker. However, the ip.buffer does not use OpenSSL.

Affects: N/A

Status: Non-exploit

ShellShock CVE-2014-6271

Info: The ip.buffer is not running Linux/Unix, does not have a shell, does not use bash.

Affects: N/A

Status: Non-exploit

POODLE attack on SSLv3 CVE-2014-3566

Info: Potential disclosure of information is possible, but requires a Man-In-The-Middle attack. There is limited opportunity to use this attack in the ip.buffer See https://polarssl.org/tech-updates/blog/sslv3-and-poodle-in-perspective

Affects: all

Status: You should limit your server to only use TLSv1, TLSv1.1 and TLSv1.2. Firmware 2.91 provides the ability to disable SSLv3 in the ip.buffer completely with the following configuration line:

```
   c.certs.sslmin=1
```

Denial of Service against GCM-enabled entities

Info: Using GCM-enable cipher suite entities, as either server or client, can cause an ip.buffer reboot due issue in PolarSSL <= 1.3.7

Affects: Firmware <= 2.90 (contains PolarSSL 1.3.7)

Status: Disable GCM entities with the following configuration line:

```
   c.certs.ciphers = '-gcm'
```

Or upgrade to firmware >= 2.91 (contains PolarSSL 1.3.9)

RTOS / Operating System Security

Info: The ip.buffer uses Green Hills Software's INTEGRITY RTOS that "*is built around a partitioning architecture to provide embedded systems with total reliability, absolute security, and maximum real-time performance*." See: http://www.ghs.com

(Additionally the ip.buffer firmware is built as a monolithic encrypted image. No part of the ip.buffer firmware can be separately updated, or modified.)

Status: There are zero vulnerabilities in the National Vulnerability Database for INTEGRITY.