

# Silver Peak Security Advisory

libpng Exploit Vulnerability, Published by NIST on 02/27/2014

CVE-2014-0333

## Summary:

US-CERT/NIST advisory for CVE-2014-0333 is dated 02/27/2014. The advisory is about a problem in libpng that can be exploited by a specially crafted file to put it into an infinite loop. The CVE database lists this as network exploitable, but only as a denial-of-service.

The png\_push\_read\_chunk function in pngpread.c in the progressive decoder in libpng 1.6.x through 1.6.9 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via an IDAT chunk with a length of zero.

**Silver Peak VXOA appliances are not susceptible to this vulnerability.**

**As an additional step, the Silver Peak VXOA appliance image will not carry libpng on the image releases specified under the heading, Resolution.**

## Details:

CVE provides information on the advisory and is located at:

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0333>

The full advisory located at <http://cwe.mitre.org/data/definitions/835.html> reads as follows:

+ Description

Description Summary

The program contains an iteration or loop with an exit condition that cannot be reached, i.e., an infinite loop.

Extended Description

If the loop can be influenced by an attacker, this weakness could allow attackers to consume excessive resources such as CPU or memory.

+ Applicable Platforms

Languages

Language-independent

+ Common Consequences

Scope Effect

Availability

Technical Impact: DoS: resource consumption (CPU); DoS: resource consumption (memory);  
DoS: amplification

An infinite loop will cause unexpected consumption of resources, such as CPU cycles or memory. The software's operation may slow down, or cause a long time to respond.

**NIST has added the vulnerability summary for this CVE to their National Cyber Awareness System database:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0333>

### **Recommended Action for Silver Peak Customers:**

**Silver Peak VXOA appliances:**

Silver Peak VXOA appliances are not affected by this vulnerability.

**Silver Peak VXOA appliances are not susceptible to this vulnerability; although libpng exists in the code, it is not used by the VXOA software.**

**As an additional step, the Silver Peak VXOA appliance image will not carry libpng on image releases specified under RESOLUTION, below.**

### **Resolution:**

Silver Peak Issue Id 24480 tracks this vulnerability.

The resolution for this vulnerability is in each of the following release branches:

- VXOA 6.2.7.0 and later releases
- VXOA 7.1.1.0 and later releases
- VXOA 7.2.0.0 and later releases