Silver Peak Security Advisory
Cross-Site Scripting (XSS) Vulnerability, Published by NIST on 07/28/2014
CVE-2014-2975

Summary:
US-CERT/NIST advisory for CVE-2014-2975 is dated 07/28/2014. The advisory is about stored and reflected cross-site scripting vulnerability.

The cross-site scripting (XSS) vulnerability in php/user_account.php in Silver Peak VX before 6.2.4 allows remote attackers to inject arbitrary web script or HTML via the user_id parameter.

Silver Peak VXOA appliances are susceptible to this vulnerability, and the patch for resolving this is detailed under the heading, Resolution.

Details:
CVE provides information on the advisory and is located at:

Instances of both stored and reflected cross-site scripting vulnerabilities exist within the VX web interface.

The full advisory located at http://www.kb.cert.org/vuls/id/867980 reads as follows:

---snip---

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - CVE-2014-2975

Silver Peak VX version 6.2.2.0_47968 also contains a reflected cross-site scripting vulnerability in /php/user_account.php that can allow an attacker to inject arbitrary HTML content (including scripts) via the vulnerable query string parameter user_id.

The CVSS score below applies to the CVE-2013-2975 vulnerability.
**Impact**

An attacker can conduct a cross-site scripting or cross-site request forgery attack, which could be used for privilege escalation or to inject arbitrary HTML content (including script) into a web page presented to the user.

**Solution**

Apply an Update

Silver Peak has provided an update to fix CVE-2014-2975 in Silver Peak VX 6.2.4. CVE-2014-2974 is expected to be addressed "in the next maintenance release" according to the vendor.

---snip---

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-2014-2975](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2975)

**Recommended Action for Silver Peak Customers:**

**Silver Peak VXOA appliances:**

Silver Peak VXOA appliances are affected by this vulnerability. To mitigate risk, Silver Peak recommends upgrading VXOA appliances to the releases listed in Resolution.

**Resolution:**

Silver Peak Issue Id 26466 tracks this vulnerability.

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

- VXOA 6.2.11 and later releases
- VXOA 7.2.0 and later releases