Silver Peak Security Advisory

Cross-Site Reflect Forgery (CSRF) Vulnerability through hardcoded account, Published by NIST on 07/28/2014

CVE-2014-2974

Summary:

US-CERT/NIST advisory for CVE-2014-2974 is dated 07/28/2014. The advisory is about CSRF.

The Cross-Site Request Forgery (CSRF) vulnerability in php/user_account.php in Silver Peak VX through 6.2.4 allows remote attackers to hijack the authentication of administrators for requests that create administrative accounts.

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:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2974

Also seclists.org site has information on this vulnerability:
http://seclists.org/fulldisclosure/2015/Sep/34

The "spsadmin" account is predefined in the VX appliance, and is hidden from user account lists in the web and subshell interfaces. The account has a hardcoded password of "Silverpeak123", and cannot be logged into through the regular web interface, or the subshell over SSH. However, the account can log in via the web JSON interface, and execute JSON API calls with administrative privileges. This can include creating new users, with which an attacker may successfully log into the SSH or web interfaces, and also exploiting the Command Injection bug detailed earlier in this advisory. The following PoC details the request and credentials used to obtain a valid REST cookie:

```
[Hardcoded account login PoC]
POST /rest/json/login HTTP/1.1
Host: [host]
Content-Type: application/json; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 46

{"user":"spsadmin","password":"Silverpeak123"}
```

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

---snip start---

CWE-352: Cross-Site Request Forgery (CSRF) - CVE-2014-2974

Silver Peak VX version 6.2.2.0_47968 contains a cross-site request forgery vulnerability in /php/user_account.php that allows an unauthenticated user to create a new administrator account.

---snip end---

---snip start---

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 end---

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-2014-2974

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 26467 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**
- **VXOA 7.3.0 and later releases**