Silver Peak Security Advisory

Unauthenticated File Read Vulnerability, Published by seclists.org on 09/09/2015

Summary:

Seclists.org advisory for the Unauthenticated File Read vulnerability is dated 09/09/2015. The advisory is about how a user with access to the VX web server interface could make an unauthenticated call to a web interface function that allows them to read arbitrary files on the disk with the permission of the web server user, "apache". Two functions are affected by this vulnerability: "save_file.php" and "save_config_file.php".

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 Unauthenticated File Read vulnerability, which reads as follows:

```
==Unauthenticated File Read==
A user with the ability to access the VX web server interface may make
an unauthenticated call to a web interface function that allows them to
read arbitrary files on the disk with the permission of the web server
user "apache". Two functions are affected by this vulnerability,
"save_file.php" and "save_config_file.php".
[Unauthenticated File Read PoC]
curl -sk
"https://[HOST]/6.2.5.0_52054/php/save_file.php?ftype=log&fname=../../etc/pas
swd";

OR

curl -sk
"https://[HOST]/6.2.5.0_52054/php/save_config_file.php?filename=../../../../.
./../../etc/passwd";
```

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 26463 tracks this vulnerability.

The resolution for this vulnerability is in the following release branch:

- **VXOA 6.2.11.0 and later releases**

VXOA 7.2.0 and later releases do not have the php files mentioned in this advisory, and thus are not susceptible to this vulnerability.