Silver Peak Security Advisory

Command Injection Vulnerability, Published by seclists.org on 09/09/2015

Summary:

Seclists.org advisory for Command Injection vulnerability is dated 09/09/2015. The advisory is about vulnerability through which a user a user with administrative access to the REST JSON interface of the VX web server may execute arbitrary commands on the operating system.

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 Command Injection vulnerability, which reads as follows:

```
==Command Injection==
A user with administrative access to the REST JSON interface of the VX
web server may execute arbitrary commands on the operating system. The
injection point lies in the "snmp" call, which does not sanitise the
"auth_key" parameter before including it in an executed command string.
The following command injection PoC writes the user's id to a file on
the filesystem.
[Command Injection PoC]
POST /rest/json/snmp HTTP/1.1
Host: [HOST]
Content-Type: application/json; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 368
Cookie: connect.sid=[VALID];

{"access":{"rocommunity":"public"},"listen":{"enable":true},"traps":{"trap_co
mmunity":"public","enable":true},"auto_launch":true,"sysdescr":"",
"syscontact":"","syslocation":"","v3":{"users":{"admin":{"hash_type":"sha","a
uth_key":"a;echo
`id` >
/var/tmp/cmd_inj","self":"admin","privacy_key":"","privacy_type":"aes-
128","enable":false}}},"encAuth":false,"encPri":false}
```

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 26462 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 7.2.1.0 and later releases**
- **VXOA 7.3.0.0 and later releases**