Silver Peak Security Advisory

Mass Assignment Vulnerability, Published by seclists.org on 09/09/2015

Summary:

Seclists.org advisory for Mass Assignment vulnerability is dated 09/09/2015. The advisory is about how a user with access to the REST JSON interface of the VX web server could alter undocumented parameters of the "users" call, allowing them to change a user's login shell to bash. This can be used to evade the limited subshell enforced by the SSH server on the appliance.

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 Mass Assignment vulnerability, which reads as follows:

```
==Mass Assignment==
A user with access to the REST JSON interface of the VX web server may
alter undocumented parameters of the "users" call, allowing them to
change a user's login shell to bash. This can be used to evade the
limited subshell enforced by the SSH server on the appliance.
[Mass assignment PoC]
POST /rest/json/users HTTP/1.1
Host: [HOST]
Content-Type: application/json; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 366
Cookie: connect.sid=[VALID];

{"users":{"basic":{"self":"basic","enable":true,"gid":0,"password":"[SNIP]","
shell":"/bin/bash"}},[SNIP
other users]}}
```

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 26464 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**