Silver Peak Security Advisory

Notification

Security Advisory 2022-01-28-01-001: Local Privilege Escalation in polkit's pkexec

Date: 01/28/2022

CVE ID: CVE-2021-4034

Vulnerability Type: CWE-284: Improper access control

Summary

The Qualys Research Team has discovered a memory corruption vulnerability in polkit's pkexec, a SUID-root program installed in many major Linux distributions. Exploitation of this vulnerability allows for any unprivileged local user to gain full root privileges on the affected host. Remote attack is not possible with this vulnerability.

Applicability to Silver Peak Products

Silver Peak Products	Applicability
Unity EdgeConnect, NX, VX	Not Applicable
EdgeConnect in Public Cloud	Not Applicable
Unity Orchestrator (self-hosted, private cloud)	Applicable
Unity Orchestrator (self-hosted, public cloud)	Applicable
Silver Peak Cloud Services: • Orchestrator-SP • Orchestrator-GE • Orchestrator-as-a-Service	Not Applicable

Recommended Action for Silver Peak Customers

All customers with self-hosted Orchestrators must perform the following actions based on their deployed configuration.
Starting with Orchestrator 9.0.6, all subsequent Orchestrator application upgrades will require the user to update their Linux OS.

Linux OS distribution	Orchestrator Release	Recommended Action
Fedora OS	doesn't matter	Security updates for Fedora are not available. See Note 1.
CentOS 7	< 9.0.6	run `yum update polkit` on the underlying Linux host. See Notes 2, 3.
CentOS 7	≥ 9.0.6	Run yum update polkit or Upgrade Orchestrator See Note 4.

Note 1: Security updates for Fedora OS are not available. Silver Peak recommends moving to CentOS by deploying a new OVA by first backing up Orchestrator, build a new one from OVA, restore configuration from backup.
Silver Peak Technical Assistance Center (TAC) can help with this procedure. It is important that only one Orchestrator can be active.

Note 2: After the yum update, proper versions should be as follows:

```
-bash-4.2# rpm -q --changelog polkit | grep CVE-2021-4034
Resolves: CVE-2021-4034
```
this indicates polkit is patched for this CVE.

```
-bash-4.2# rpm -qa | grep -i polkit
polkit-pkla-compat-0.1-4.el7.x86_64
polkit-0.112-26.el7_9.1.x86_64
```
this also indicates that the host is on a MINIMUM version that has the patch for CVE-2021-4034.

Note 3: An Orchestrator application upgrade is not required to address CVE-2021-4034.

Note 4: Users can simply run yum update or update the Orchestrator application which requires the user to run yum update.

References

Details about the vulnerability are published at:

https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

Thank you,

Product Security Incident Response Team at Silver Peak