Silver Peak Security Advisory

Notification

Dirty COW Vulnerability

Dirty COW is a privilege escalation vulnerability in the Linux Kernel

CVE-2016-5195 published by dirtycow.ninja on October 21, 2016

Summary:

This is a Linux kernel security advisory for CVE-2016-5195.

The issue CVE-2016-5195 states that:
A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

The Silver Peak appliance is a hardened embedded system and not a multi-user general purpose Linux operating system. So the privilege escalation resulting from Dirty COW is “very low”, in its applicability to Silver Peak deployments. Based on this, and based on the CVSS 3.0 score of 7.8, we would not issue a patch or fix at this time.

Applicability to Silver Peak deployments: Low

(**Includes Silver Peak VXOA release for NX/VX/VRX/CPX/EdgeConnect appliances)**

Recommended Action for Silver Peak Customers:

Silver Peak VXOA release for NX/VX/VRX/CPX/EdgeConnect appliances:
No action required

Silver Peak Unity Orchestrator/GMS IS susceptible to this vulnerability.

Silver Peak GMS / Unity Orchestrator: A kernel update fixes the issue for the Orchestrator. Please refer to the Orchestrator 8.2.2 release notes for more details on how to do this.

Resolution:

Upgrade kernel on the Orchestrator

Details:

The full details of the advisory are located at-

https://dirtycow.ninja/

Thank you.

Security Incident Response Team

Silver Peak