

Silver Peak Security Advisory

Notification

Security Advisory 2020-12-11-01-002: OS Command Injection - Management File Upload

CVE ID: CVE-2020-12149

Vulnerability Type: [CWE-78](#): Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Details

The configuration backup/restore function in Silver Peak Unity ECOS™ (ECOS) appliance software was found to directly incorporate the user-controlled config filename in a subsequent shell command, allowing an attacker to manipulate the resulting command by injecting valid OS command input. This vulnerability can be exploited by an attacker with authenticated access to the Orchestrator UI or EdgeConnect UI.

Affected Versions

All ECOS versions **prior to** 8.1.9.15, 8.3.0.8, 8.3.1.2, 8.3.2.0, 9.0.2.0, and 9.1.0.0 are affected.

Resolution

The backup/restore functions in the patched versions of ECOS software have been modified to only accept alphanumeric characters, along with the period, hyphen, and underscore characters. This change ensures that OS commands cannot be injected via filename.

Recommended Actions for Silver Peak Customers

Upgrade EdgeConnect appliance software to ECOS 8.1.9.15+, 8.3.0.8+, 8.3.1.2+, 8.3.2.0+, 9.0.2.0+, or 9.1.0.0+.

Applicability to Silver Peak Products

Silver Peak Products	Applicability
Unity EdgeConnect, NX, VX	Applicable
EdgeConnect in Public Cloud	Applicable
Unity Orchestrator	Not Applicable
Silver Peak Cloud Services	Not Applicable

Common Vulnerability Impact Rating

<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H>

6.8
(Medium)

Base Score

Attack Vector (AV)	Scope (S)
<input checked="" type="radio"/> Network (N) <input type="radio"/> Adjacent (A) <input type="radio"/> Local (L) <input type="radio"/> Physical (P)	<input checked="" type="radio"/> Unchanged (U) <input type="radio"/> Changed (C)
Attack Complexity (AC)	Confidentiality (C)
<input checked="" type="radio"/> Low (L) <input type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)
Privileges Required (PR)	Integrity (I)
<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)
User Interaction (UI)	Availability (A)
<input type="radio"/> None (N) <input checked="" type="radio"/> Required (R)	<input type="radio"/> None (N) <input type="radio"/> Low (L) <input checked="" type="radio"/> High (H)

Attestation

This vulnerability was reported to Silver Peak by Alexander Smye from the security team at NCC Group.

References

The full details of the CVE can be found [here](#).

Thank you,
Product Security Incident Response Team at Silver Peak