Silver Peak Security Advisory

Notification

Security Advisory 2020-12-11-01-001: OS Command Injection - nslookup API

CVE ID: CVE-2020-12148

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

Details

A command injection flaw identified in the nslookup API in Silver Peak Unity ECOS™ (ECOS) appliance software could allow an attacker to execute arbitrary commands with the privileges of the web server running on the EdgeConnect appliance. An attacker could exploit this vulnerability to establish an interactive channel, effectively taking control of the target system. 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

In the patched ECOS versions, the APIs 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 the API.

Recommended Actions for Silver Peak Customers

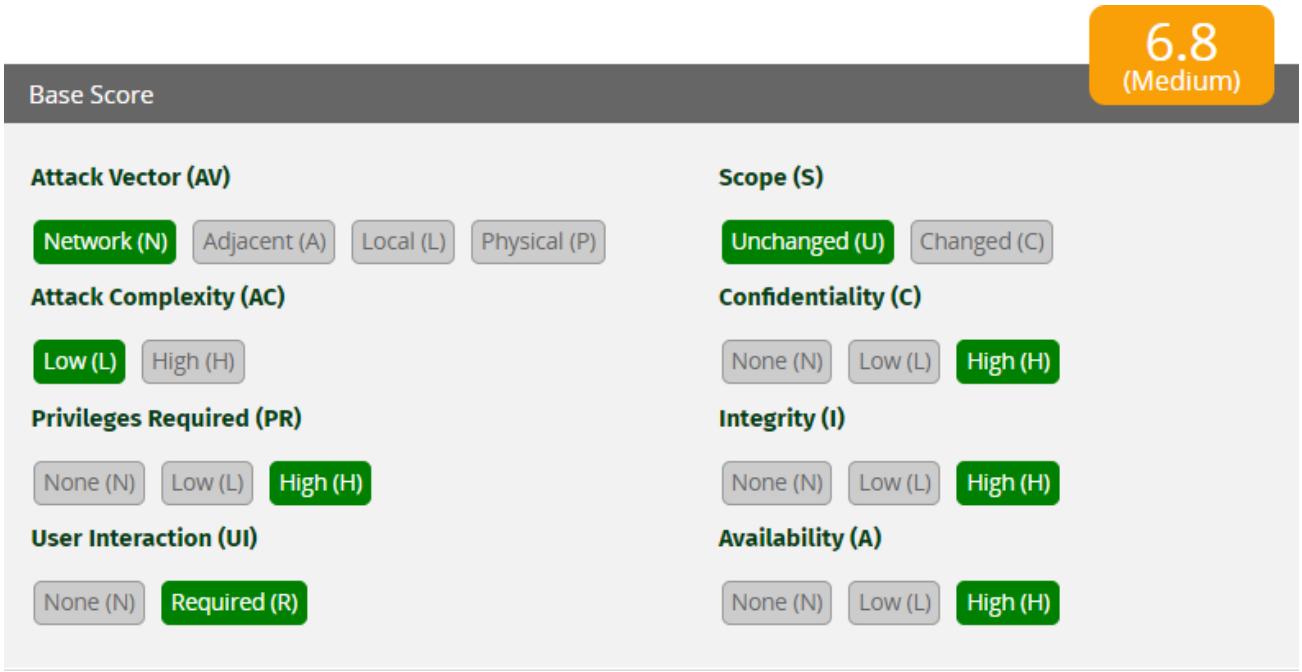
Upgrade EdgeConnect appliance software to ECOS 8.1.9.15+, 8.3.0.8+, 8.3.1.2+, 8.3.2.0+, 9.0.2.0+, or 9.1.0.0+.

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



Attestation

This vulnerability was reported to Silver Peak by Alexander Smye and Jonathan Letham 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