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 ECOSTM (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

<table>
<thead>
<tr>
<th>Silver Peak Products</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unity EdgeConnect, NX, VX</td>
<td>Applicable</td>
</tr>
<tr>
<td>EdgeConnect in Public Cloud</td>
<td>Applicable</td>
</tr>
<tr>
<td>Unity Orchestrator</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Silver Peak Cloud Services</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
**Common Vulnerability Impact Rating**


**Attestation**

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

**References**


Thank you,

Product Security Incident Response Team at Silver Peak