Systems vulnerable to Supernova malware

Your company uses SolarWinds Orion business software, which is vulnerable to the Supernova in-memory web shell attack. You know that because it runs in memory, detection and forensic analysis post-breach are difficult. You want to identify vulnerable systems as soon as possible.

Required data

- Vulnerability scanning data

Option 1 - Normalized data

1. Ensure that your deployment is ingesting endpoint logs from your various systems and populating the Vulnerabilities data model.
2. Ensure that you have a recent vulnerability scan (such as from Tenable, Qualsys, or Acunetix) with the SolarWinds Orion API vulnerability alert added.
3. Run the following search. You can optimize it by specifying an index and adjusting the time range.

| tstats count FROM datamodel=Vulnerabilities.Vulnerabilities WHERE Vulnerabilities.cert=VU#843464 OR Vulnerabilities.cert=843464 OR Vulnerabilities.cve=CVE-2020-10148 groupby Vulnerabilities.dest Vulnerabilities.dvc Vulnerabilities.signature Vulnerabilities.vendor_product _time span=1s

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>tstats count FROM datamodel=Vulnerabilities.Vulnerabilities WHERE Vulnerabilities.cert=VU#843464 OR Vulnerabilities.cert=843464 OR Vulnerabilities.cve=CVE-2020-10148 groupby Vulnerabilities.dest Vulnerabilities.dvc Vulnerabilities.signature Vulnerabilities.vendor_product _time span=1s</td>
<td>Query the Vulnerabilities data model for strings that correspond to the US Computer Emergency Readiness (CERT) identifier or from the Common Vulnerabilities Exposures index (CVE) that have been identified with the attack of interest, in this case the SolarWinds attack.</td>
</tr>
</tbody>
</table>
Option 2 - Without normalized data

To optimize the search shown below, you should specify an index and a time range.

1. Ensure that you have a recent vulnerability scan (such as from Tenable, Qualsys, or Acunetix) with the SolarWinds Orion API vulnerability alert added.
2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   sourceType=<vulnerability scanner> (VU#843464 OR 843464 OR CVE-2020-10148)
   | stats count BY dest host signature vendor _time

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceType=&lt;vulnerability scanner&gt;</td>
<td>Search only data from your vulnerability scanner.</td>
</tr>
<tr>
<td>(VU#843464 OR 843464 OR CVE-2020-10148)</td>
<td>Filter on strings that correspond to the US Computer Emergency Readiness (CERT) identifier or from the Common Vulnerabilities Exposures index (CVE) that have been identified with the attack of interest, in this case the SolarWinds attack.</td>
</tr>
<tr>
<td></td>
<td>stats count BY dest host signature vendor _time</td>
</tr>
</tbody>
</table>

Next steps

You can refine this search further based on IP address or other attributes. The searches provide a table showing the destination, device, signature, the vulnerability vendor that produced the entry as a result of a scan, the time and the count. The destination is the host where the vulnerability was found and should be the focus of your vulnerability response action plan. A response typically includes collecting evidence for forensics and then removing the malware and making sure the vulnerability is remediated.

Finally, you might be interested in other processes associated with the Detecting Supernova web shell malware use case.