Identify SolarWinds Vulnerability Risk.

Fact sheet

SolarWinds Compromise Rapid Assessment

On December 13, 2020, SolarWinds announced that specific versions of the SolarWinds Orion Platform were subject to a vulnerability where malicious code was added to their software by an advanced adversary.

This vulnerability has been labeled the SUNBURST backdoor by FireEye. If present and activated in customer environments, the backdoor could potentially allow an attacker to gain unauthorized access to the Solarwinds Server.

Verizon's SolarWinds Compromise Rapid Assessment:

- Determines whether in-scope systems were subject to the vulnerability
- Provides an independent third-party validation associated with the risk and potential impacts of the vulnerability
- Provides findings and recommendations on actions to take for response and mitigation

How it works.

Verizon provides:

- Remote guidance on collecting in-scope Source Artifacts, specifically DNS logs and the malicious DLL (as applicable)
- On-boarding and preparation of in-scope Source Artifact items and conducting of the Assessment
- Findings specific to whether a vulnerability exists and whether the vulnerability was or may be exploited
- Advice on any containment, eradication, remediation, or recovery measures

This assessment is completely virtual – with data collection conducted from the cloud – and can be completed in as little as one day. Verizon recommends that all servers with SolarWinds instances be assessed.

Reporting

Verizon analyzes all of the data collected during the operation and generates a single report detailing findings including an indication of whether the risk that the SolarWinds instance(s) was subject to the SUNBURST backdoor vulnerability is low, medium or high. If a medium or high risk is found, Verizon recommends further investigation of potential unauthorized activity.

Learn more.

Verizon SolarWinds Compromise Rapid Assessment will help improve your security posture by determining if you have the SolarWinds vulnerability risk. For more information, speak to your Verizon Account Manager.

Current Version	Previous Version	C2 DNS Queries
• What is the current version installed in the environment?	• What was the previous version installed in the environment?	• DNS queries to the known Command-and-Control (C2) infrastructure?
• Is the current version impacted by the vulnerability?	• Was the previous version impacted by the vulnerability?	• Were those DNS queries successful or unsuccessful?

verizon