SOLARWINDS ORION COMPROMISE

SUNBURST EXPOSURE ASSESSMENT

OVERVIEW

In response to the SolarWinds Orion breach, we, as a community, have had to rapidly respond to the related breach and data exfiltration. The attackers behind this campaign have gained access to numerous public and private organizations around the world. The malware is designed to masquerade and blend in, allowing its operators to move laterally and discreetly through your environment.

RedSeal recently released a high-level overview of how to leverage our product to assist in your investigation, containment, and remediation efforts following the recent activity impacting SolarWinds Orion. The playbook questions are:

Step 1: Where is SolarWinds Orion, in context of my network?

Step 2: What is it (Orion) capable of accessing/controlling?

Step 3: Fix Orion or take it offline (if subject to the CISA Emergency Directive).

Step 4: Block unwanted access to or from SolarWinds Orion, to the extent possible.

Step 5: For all assets SolarWinds could reach, reset them to known good state.

We know this is a difficult situation, so RedSeal is offering a complementary Sunburst Exposure Assessment for our customers to help guide and prioritize remediation efforts. The Assessment includes the following actions:

1. Locate SolarWinds Orion

A RedSeal Professional Services engineer will consult with you and your internal stakeholders to identify and locate SolarWinds Orion devices on your network, using vulnerability scan data or endpoint data ingested into RedSeal.

2. Determine what access there is to/from SolarWinds Orion

The engineer will consult with you and your internal stakeholders to determine access to and from your SolarWinds Orion server using inbound, outbound, access, and threat queries.

From here you can determine the best path forward to block traffic or disable SolarWinds altogether.

3. List all assets SolarWinds Orion can access for prioritized remediation

The engineer will use RedSeal with you and your internal stakeholders to visualize and determine what devices SolarWinds Orion has direct access to, so you can prioritize remediation efforts. The data in RedSeal will also determine immediate and pivotable access. We recommend resetting all assets SolarWinds can reach to a known good state.

4. Verify network device configurations using custom checks

The engineer will consult with you and your internal stakeholders to develop up to five custom checks for your network environment. You'll be able to use these checks to verify network device configurations, routing configurations, or track credential changes on network devices. You'll be able to track device resetting, enable stronger protection methods, and verify security settings.