SolarWinds Security Advisory

Recent as of April 6, 2021, 9:00am CST

This page covers the SolarWinds response to both SUNBURST and SUPERNOVA, and the steps we are taking in response to these incidents.

- For information about **SUNBURST**, go here.
- For information about **SUPERNOVA**, go here.
- For information about our new digital code-signing certificate, go here.

We continue to strive for transparency and keeping our customers informed to the extent possible as we cooperate with law enforcement and intelligence communities, and to the extent it is in the best interest of our customers. Like other software companies, we seek to responsibly disclose vulnerabilities in our products to our customers while also mitigating the risk that bad actors seek to exploit those vulnerabilities by releasing updates to our products that remediate these vulnerabilities before we disclose them.

For the latest update on our investigation, please read this blog, and to learn more about the steps we're taking to ensure the security and performance of the products we deliver, go here. You can also to be notified when we update this page (note: you will need to cut and paste the "Subscribe to this RSS feed" URL into an RSS Feed Reader, e.g. Outlook's RSS Subscriptions, to monitor updates).

A detailed Frequently Asked Questions (FAQ) page is available here, and we intend to update this page as we learn more information.

ABOUT OUR NEW DIGITAL CODE-SIGNING CERTIFICATE

As announced by SolarWinds President and CEO Sudhakar Ramakrishna in his Orange Matter blog, *Our Plan for a Safer SolarWinds and Customer Community*, we're taking key steps to ensure the security and integrity of the software we deliver to customers.

SolarWinds uses a digital code-signing certificate to digitally sign each software build, and to help end users authenticate the code comes from us. As part of our response to the SUNBURST vulnerability, the code-signing certificate used by SolarWinds to sign the affected software versions was revoked **March 8, 2021. This is industry-standard best practice for software that has been compromised.**

We've obtained new digital code-signing certificates and have rebuilt the versions signed with the certificate to be revoked, have re-signed our code, and have re-released all of the products previously signed with the certificate to be revoked. To ensure the performance of your SolarWinds product(s), you must upgrade to these new builds.

For full details on this part of our response to the SUNBURST vulnerability, please visit our **SolarWinds New Digital Code-Signing Certificate** page at solarwinds.com/trust-center/new-digital-certificate.

ABOUT SUPERNOVA

SUPERNOVA is malware that was deployed using a vulnerability in the Orion Platform, and after the Orion Platform had been installed. Based on our investigation to date:

- SUPERNOVA is not malicious code embedded within the builds of our Orion® Platform as a supply chain attack. It is malware that is separately placed on a server that requires unauthorized access to a customer's network and is designed to appear to be part of a SolarWinds product.
- The SUPERNOVA malware consisted of two components. The first was a malicious, unsigned webshell .dll "app_web_logoimagehandler.ashx.b6031896.dll" specifically written to be used on the SolarWinds Orion Platform. The second is the utilization of a vulnerability in the Orion Platform to enable deployment of the malicious code. This vulnerability in the Orion Platform has been resolved in the latest updates.

We constantly work to enhance the security of our products and to protect our customers and ourselves because hackers and other cybercriminals are always seeking new ways to find and attack their victims. We work closely with our customers to address and remediate any potential concerns, and we encourage all customers to run only supported versions of our products and to upgrade to the latest versions to the get the full benefit of our updates, improvements, and enhancements.

ABOUT SUNBURST

SolarWinds and our customers were the victims of a cyberattack to our systems that inserted a vulnerability (SUNBURST) within our Orion® Platform software builds for versions **2019.4 HF 5, 2020.2 unpatched,** and **2020.2 HF 1**, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. This attack was a very sophisticated supply chain attack, which refers to a disruption in a standard process resulting in a compromised result with a goal of being able to attack subsequent users of the software. In this case, it appears that the code was intended to be used in a targeted way as its exploitation requires manual intervention. We've been advised that the nature of this attack indicates that it may have been conducted by an outside nation state, but SolarWinds has not verified the identity of the attacker.

As our investigation has progressed, and as we've worked with CrowdStrike and KPMG, we've identified malware known as SUNSPOT, the highly sophisticated and novel code designed to inject the SUNBURST malicious code into the Orion Platform during the build process. SUNSPOT is not a new malware or attack, but instead a component of the SUNBURST cyberattack. Read more about SUNSPOT on the CrowdStrike blog here.

While SUNSPOT is the means by which the attackers injected the SUNBURST backdoor during the build process of the Orion Platform, TEARDROP and RAINDROP are reportedly malware loaders that could be deployed as secondary tools using the SUNBURST backdoor. SUNSPOT, TEARDROP, and RAINDROP **are NOT new vulnerabilities** within our products as some reports in the media have indicated, but instead, they **are elements of the SUNBURST attack chain**.

The Cybersecurity and Infrastructure Security Agency (CISA) Computer Emergency Readiness Team (CERT), part of the Department of Homeland Security (DHS), CERT issued Emergency Directive 21-01 on December 13, 2020 regarding this issue and has updated their guidance as part of our ongoing coordination with the agency. The latest information can be found on CISA's Supply Chain Compromise page and continues to be updated as we learn more.

We want to assure you we've removed the software builds known to be affected by the SUNBURST vulnerability from our download sites.

While our investigations are ongoing, based on our investigations to date, we are not aware that this SUNBURST vulnerability affects other versions of Orion Platform products. Also, while we are still investigating our non-Orion products, we have not seen any evidence that they are impacted by the SUNBURST vulnerability.

If you aren't sure which version of the Orion Platform you are using, see directions on how to check that here. To check which hotfix updates you have applied, please go here.

Known affected products: Orion Platform versions **2019.4 HF 5, 2020.2 with no hotfix installed, or with 2020.2 HF 1**, including:

- Application Centric Monitor (ACM)
- Database Performance Analyzer **Integration Module*** (DPAIM*)
- Enterprise Operations Console (EOC)
- High Availability (HA)
- IP Address Manager (IPAM)
- Log Analyzer (LA)
- Network Automation Manager (NAM)
- Network Configuration Manager (NCM)
- Network Operations Manager (NOM)
- User Device Tracker (UDT)
- Network Performance Monitor (NPM)
- NetFlow Traffic Analyzer (NTA)
- Server & Application Monitor (SAM)
- Server Configuration Monitor (SCM)
- Storage Resource Monitor (SRM)
- Virtualization Manager (VMAN)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)

***NOTE:** Please note DPAIM is an integration module and **is not the same** as Database Performance Analyzer (DPA), which we do not believe is affected.

SolarWinds products **NOT KNOWN TO BE AFFECTED** by this security vulnerability:

- 8Man
- Access Rights Manager (ARM)
- AppOptics
- Backup Document
- Backup Profiler
- Backup Server
- Backup Workstation
- CatTools
- Dameware Mini Remote Control
- Dameware Patch Manager
- Dameware Remote Everywhere
- Dameware Remote Manager
- Database Performance Analyzer (DPA)
- Database Performance Monitor (DPM)
- DNSstuff
- Engineer’s Toolset
- Engineer's Web Toolset
- FailOver Engine
- Firewall Security Monitor
- Identity Monitor
- ipMonitor
- Kiwi CatTools
- Kiwi Log Viewer
- Kiwi Syslog Server
- LANSurveyor
- Service Desk
- Serv-U FTP Server
- Serv-U Gateway
- Serv-U MFT Server
- Storage Manager
- Storage Profiler
- Threat Monitor
- Virtualization Profiler
- Web Help Desk
- SQL Sentry
- DB Sentry
- V Sentry
- Win Sentry
- BI Sentry
- SentryOne Document
- SentryOne Test
- Task Factory
- DBA xPress
- Plan Explorer
- APS Sentry
- DW Sentry
- SQL Sentry Essentials
- SentryOne Monitor
- BI xPress

Librato	**SolarWinds MSP Products:**
Log & Event Manager (LEM)	N-central – Probe
Log and Event Manager Workstation Edition	N-central – Topology
Loggly	N-central – NetPath
Mobile Admin	N-central
Network Topology Mapper (NTM)	NetPath – Server
Papertrail	RMM
Patch Manager	Backup Disaster Recovery
Pingdom	M365 Backup
Pingdom Server Monitor	Backup
Security Event Manager (SEM)	Mail Assure
Security Event Manager Workstation Edition	SpamExperts
Server Profiler	MSP Manager
	PassPortal
	Take Control
	Patch
	Automation Manager
	Webprotection

We have also found no evidence that any of our free tools, Orion agents, or Web Performance Monitor (WPM) Players are impacted by SUNBURST.

RECOMMENDED ACTIONS

SolarWinds uses a digital code-signing certificate to digitally sign each software build, and to help end users authenticate the code comes from us. As part of our response to the SUNBURST vulnerability, the code-signing certificate used by SolarWinds to sign the affected software versions was revoked **March 8, 2021. This is industry-standard best practice for software that has been compromised.**

We've obtained new digital code-signing certificates and have rebuilt the affected versions, have re-signed our code, and have re-released all of the products previously signed with the certificate to be revoked. To ensure the performance of your SolarWinds product(s), you must upgrade to these new builds.

If you're unable to upgrade at this time, we have provided a script that customers can install to temporarily protect their environment against the SUPERNOVA malware***. The script is available at https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip.

To take advantage of our latest available security updates protections for the products you have deployed, we recommend all active maintenance customers of Orion Platform products **upgrade to version 2020.2.5** as soon as possible. For more information, review the Release Notes here, and KB article here.

Customers on **Orion Platform versions 2019.4.2 or 2020.2.4** have applied security enhancements designed to protect you from SUNBURST and SUPERNOVA. **NOTE:** If you reinstall, you need to re-apply the patch or hotfix.

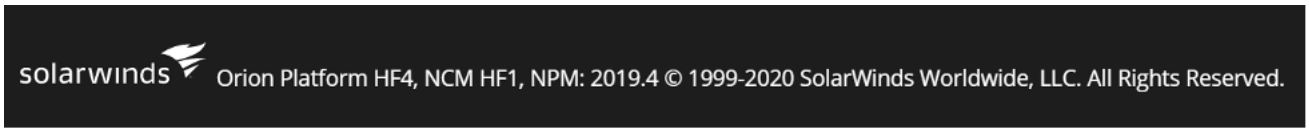
The latest updates designed to protect against SUNBURST and SUPERNOVA are as follows:

- 2019.2 HF 4 (released February 5, 2021)
- 2019.4.2 (released February 2, 2021)
- 2020.2.4 (released January 25, 2021)
- 2019.2 Security Patch (released December 23, 2020)
- 2018.4 Security Patch (released December 23, 2020)
- 2018.2 Security Patch (released December 23, 2020)

To identify the version of the Orion Platform software you are using, you can review the directions on how to check here or refer to the image below. To check which updates you have applied, please go here.

From Orion Web Console

All product versions are displayed in the footer of the Orion Web Console login page. See the example below of **2019.4 HF 4**:



We recommend taking the steps related to your use of your version of the SolarWinds Orion Platform per the table below:

Orion Platform Version	Known Affected by SUNBURST?	Known Vulnerable to SUPERNOVA?	Affected by Digital Certificate Revocation	Recommended Action	Direct Link
2020.2.5	**NO**	**NO**	**NO**	**No action needed**	**No action needed**
2020.2.4	**NO**	**NO**	**NO**	**No action needed to protect against SUNBURST or SUPERNOVA; though SolarWinds recommends you upgrade to 2020.2.5 to address other, unrelated security vulnerabilities. More info is here.**	**customerportal.solarwinds.com**
2020.2.1 HF 2	**NO**	**NO**	**YES**	**Upgrade to 2020.2.5**	**customerportal.solarwinds.com**
2020.2.1 HF 1	**NO**	**YES**	**YES**	**Upgrade to 2020.2.5**	**customerportal.solarwinds.com**
2020.2.1	**NO**	**YES**	**YES**	**Upgrade to 2020.2.5**	**customerportal.solarwinds.com**
2020.2 HF 1	**YES**	**YES**	**YES**	**Upgrade to 2020.2.5**	**customerportal.solarwinds.com**

2020.2	**YES**	**YES**	**YES**	**Upgrade to 2020.2.5**	**customerportal.solarwinds.com**
2019.4.2	**NO**	**NO**	**NO**	**No action needed**	**No action needed**
2019.4 HF 6	**NO**	**NO**	**YES**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4 HF 5	**YES**	**YES**	**YES**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4 HF 4	**NO**	**YES**	**YES**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4 HF 3	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4 HF 2	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4 HF 1	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.4	**NO***	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.2 HF 3	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.2 HF 2	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.2 HF 1	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2019.2	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
2018.4	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**

2018.2	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5** OR **upgrade to 2019.4.2**	**customerportal.solarwinds.com**
All prior versions	**NO**	**YES**	**NO**	**Upgrade to 2020.2.5, apply temporary mitigation script, or discontinue use**	To upgrade, go to **customerportal.solarwinds.com** OR to apply t mitigation script*** go to **https://downloads.solarwinds.com/solarwinds/Support/Superı**

*As a part of the ongoing investigation, we have determined that Orion Platform version 2019.4 unpatched, released in October 2019, contained test modifications to the code base. While this version is not impacted by the SUNBURST vulnerability, it is the first version in which we have seen activity from the attacker at this time. Subsequent releases 2019.4 HF 1, 2019.4 HF 2, 2019.4 HF 3, and 2019.4 HF 4 did not include either test modifications contained in the 2019.4 version or the SUNBURST vulnerability contained in 2019.4 HF 5, 2020.2 with no hotfix and 2020.2 HF 1.

** If you apply a SUPERNOVA security patch per the above chart, please visit this KB article to validate the patch was applied to all Orion Platform web servers. If you reinstall your Orion server, you will need to reapply the respective patch.

*** If you use the SUPERNOVA Mitigation Script to address the SUPERNOVA vulnerability, use the guidance in the document within that package to confirm the temporary patch. Please note that this script has only been tested down to NPM 11.x. If you reinstall your Orion server, you will need to reapply this script.

All recommended upgrade versions are currently available at customerportal.solarwinds.com.

All hotfix updates are cumulative and can be installed from any earlier version. There is no need to install previously released hotfix updates. **You may need to synchronize your license prior to applying the hotfix.** Please follow the steps here to kick off the synchronization of your license.

If you have disabled outward communication from your Orion license, please follow the “Activate License Offline” section from here. Once you have successfully synched your license, please run the installer to install the hotfix.

To provide additional security for your Orion Platform installation, please follow the guidelines available here for your Orion Platform instance. The primary mitigation steps include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform, and limiting the ports and connections to only what is required to operate your platform.

WHAT ARE WE DOING TO HELP?

Our primary focus has been on helping our customers protect the security of their environments. Our commitment to our customers remains high, and we’ve introduced a new program designed to address the issues our customers face.

We’ve developed a program to provide professional consulting resources experienced with the Orion Platform and products to assist customers who need guidance on or support upgrading to the latest hotfix updates. **These consulting services will be provided at no charge to our active maintenance Orion Platform product customers.** We want to make sure that customers working to secure their environments have the help and assistance they need from knowledgeable resources. Read more about the program here.

We continue to work with leading security experts in our investigations to help further secure our products and internal systems.

SUMMARY

Security and trust in our software is the foundation of our commitment to our customers. We strive to implement and maintain appropriate administrative, physical, and technical safeguards, security processes, procedures, and standards designed to protect our customers.

Our investigations and remediation efforts for the SUNBURST vulnerability are early and ongoing. Thank you for your continued patience and partnership. We are making regular updates to this Security Advisory page at solarwinds.com/securityadvisory, and we encourage you to refer to this page.