Security Advisory FAQ | SolarWinds

solarwinds.com/securityadvisory/faq

QUESTION 1

Recent as of 4/6/2021

If I’ve upgraded to Orion Platform versions 2019.4.2, 2020.2.4, or 2020.2.5, am I affected by SUNBURST or SUPERNOVA?

Orion Platform versions 2019.4.2 and 2020.2.4 were designed to **protect you from both SUNBURST and SUPERNOVA—and have also been digitally re-signed with our newly obtained digital code-signing certificates.**

Orion Platform version 2020.2.5 adds to these enhancements with additional security fixes and protections. We recommend you upgrade to the latest available release (2020.2.5) as soon as is practical. For more information, review the Release Notes here, and KB article here.

If you have recently upgraded to 2020.2.1 HF2 or 2019.4 HF 6, you are **also protected from SUNBURST and SUPERNOVA**. However, 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to the SUNBURST vulnerability, the code-signing certificate used by SolarWinds to sign the affected software versions was revoked **March 8, 2021**, and you may experience performance issues if you do not apply the more recent updates. Please visit our **SolarWinds New Digital Code-Signing Certificate** page atsolarwinds.com/trust-center/new-digital-certificate for more information.

QUESTION 2

Recent as of 4/6/2021

Am I safe if I disconnect my Orion server from the internet?

Disconnecting any product from the internet can reduce your attack surface. The Orion Platform is fully functional without an internet connection. Based on our investigations to date, SUNBURST requires an internet connection to be activated and disconnecting your Orion server from the internet should immediately protect your environment from SUNBURST. The vulnerability in the product that allows for the deployment of SUPERNOVA, however, may still be exploited by a malicious actor who accesses your network from inside and not over the internet. Disconnecting from the internet will limit the ability of an external actor exploiting this vulnerability over an internet connection.

IMPORTANT NOTE: Disconnecting from the internet is not a recommended substitute for upgrading your Orion software to versions 2019.4.2, 2020.2.4, or 2020.2.5, or applying appropriate patches to older versions if a full upgrade is not possible at this time.

QUESTION 3

Recent as of 4/6/2021

How has SolarWinds addressed SUNBURST and SUPERNOVA?

We have:

- removed the software builds known to be affected by SUNBURST from our download sites;
- provided software updates, which include security enhancements, that are designed to address both SUNBURST and SUPERNOVA in supported versions of the Orion server; and
- provided a fix for customers on unsupported versions further described below.

RECOMMENDED ACTIONS

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**. Please visit our **SolarWinds New Digital Code-Signing Certificate** page atsolarwinds.com/trust-center/new-digital-certificate for more information.

We strongly encourage customers to upgrade their Orion products to the latest versions available in the Customer Portal at customerportal.solarwinds.com that are designed to protect you from SUNBURST and SUPERNOVA. Doing so allows you to the get the full benefit of our updates, improvements, and enhancements.

- If you **have** already upgraded to **2020.2.5**, additional security fixes and protections unrelated to SUNBURST and SUPERNOVA are included in this version. For more information, review the Release Notes here, and KB article here.
- If you have upgraded to **2020.2.4** or **2019.4 HF 2**, both the SUNBURST and SUPERNOVA vulnerabilities have been addressed in these versions—and they have also been digitally re-signed by newly obtained digital code-signing certificates.

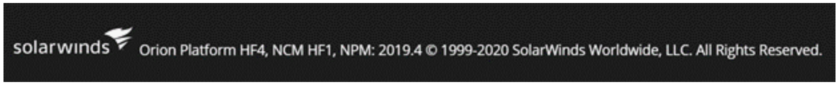
- If you **have not** already upgraded to **2020.2.5**, **2020.2.4**, or **2019.4.2**, follow the guidance identified for your current version of your Orion Platform products below to help ensure the security of your environment.

Here are the steps to take:

1. Identify the version of the Orion Platform products you are using by reviewing the directions on how to check that 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**:

   solarwinds Orion Platform HF4, NCM HF1, NPM: 2019.4 © 1999-2020 SolarWinds Worldwide, LLC. All Rights Reserved.

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

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

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 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
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/Super**

* 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 unpatched, 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 used 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 updates.

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

QUESTION 4

Recent as of 12/26/2020

Are SUNBURST and SUPERNOVA related?

While there has been speculation by various sources, based on our investigations to date, we do not have a definitive answer at this time. SolarWinds continues to work closely with federal agencies and third-party cybersecurity firms to determine the answer.

QUESTION 5

Recent as of 1/29/2021

What are SUNSPOT, TEARDROP, and RAINDROP?

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.**

SUNSPOT, for example, is the means by which the attackers injected the SUNBURST backdoor during the build process of the Orion Platform, while TEARDROP and RAINDROP are reportedly malware loaders that could be deployed using the SUNBURST backdoor.

QUESTION 6

Recent as of 1/13/2021

How is SolarWinds responding to these security vulnerabilities?

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

All new hotfixes and patches we have released since SUNBURST was detected have undergone these new levels of scrutiny. SolarWinds is increasing existing actions and taking additional actions across the enterprise to further harden and improve the security of our environment and products:

- Increased hardening of build environment and build pipeline
- Auditing and surveillance
- Environmental reviews by third-party cybersecurity experts
- Release code penetration testing (pentesting)
- Increased scanning of downloadable bits
- Scanning and analysis of source code and build output
- Refreshing of all employee and contractor credentials and credential security and elevating access restriction
- Re-signing of all release code with new certificates

In addition, we're elevating our ongoing architectural focus on continually improving the way we design, build, and support our products.

QUESTION 7

Recent as of 4/6/2021

What actions should I take?

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**. Please visit our **SolarWinds New Digital Code-Signing Certificate** page atsolarwinds.com/trust-center/new-digital-certificate for more information.

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. The latest versions of our products are available in the Customer Portal at customerportal.solarwinds.com. Based on our investigation, we recommend that all customers of Orion Platform products apply the latest updates applicable to the version of the product they have deployed.

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.

Orion Platform versions 2019.4.2 and 2020.2.4 were designed to protect you from both the SUNBURST vulnerability and the SUPERNOVA malware and have been re-signed with our newly obtained digital-signing certificate.

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.

If you're unable to upgrade at this time, we have provided a script that customers can install to temporarily protect their environment against SUPERNOVA. The script is available at https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip. If you reinstall your Orion server, you will need to reapply this script.

We also recommend customers review our **Secure Configuration for the Orion Platform** guide here for additional best practices.

QUESTION 8

Recent as of 12/15/2020

How do I know what version I'm on?

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

QUESTION 9

Recent as of 12/24/2020

How do I know if my environment was exposed?

To get started, please review the Security Advisory page on our website, as we update it with the latest information. Next, determine if your environment is at risk by verifying the version of the Orion Platform you have installed here, and verify which hotfix updates you have installed here.

Once you've determined which version you have installed, go here to see what steps you should take.

QUESTION 10

Recent as of 12/18/2020

How do I upgrade my Orion Platform version?

Please watch this video to learn more about upgrading your version of the Orion Platform software.

QUESTION 11

Recent as of 12/16/2020

My antivirus software is alerting on the of SolarWinds.Orion.Core.BusinessLayer.dll – am I infected?

We've been advised some Endpoint Security tools are alerting on **all** versions of SolarWinds.Orion.Core.BusinessLayer.dll, including versions that we do not believe were impacted by SUNBURST. We're working with those vendors to update their security definitions to eliminate these false positives.

QUESTION 12

Recent as of 4/5/2021

Some endpoint security tools flag old Orion installers left behind after upgrading to protected versions. Do these alerts mean that I am still at risk?

Not necessarily. We do not have evidence to suggest that the mere presence of these old Orion installers puts you at risk.

If you've already upgraded to 2019.4.2, 2020.2.4, or 2020.2.5, the affected SolarWinds.Orion.Core.BusinessLayer.dll was removed and replaced from the runtime area, prohibiting it from executing further. However, depending on the path taken to upgrade, some old versions of the .dll or MSIs were not fully removed.

To eliminate these alerts, we recommend that you remove those old installer files by following the steps outlined here.

QUESTION 13

Recent as of 4/6/2021

Has the Department of Homeland Security issued an Emergency Directive on this vulnerability?

Yes, 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. CERT issued Alert (AA20-352A), titled *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, as an update to ED 21-01 on December 17, 2020, based on our coordination with the agency. DHS released Supplemental Guidance to ED 21-01 on December 18, 2020, CERT revised its Alert AA20-352A on December 19, 2020, DHS released Supplemental Guidance v2 on December 30, 2020, and released Supplemental Guidance v3 on January 6, 2021 as part of our ongoing coordination with the agency. Additionally, CISA released a malware analysis report of SUPERNOVA on January 27, 2021.

The latest information can be found on the **CISA Supply Chain Compromise** page at https://www.cisa.gov/supply-chain-compromise.

The latest release, Orion Platform version **2020.2.5** is now available in the SolarWinds Customer Portal at customerportal.solarwinds.com, in accordance with ED 21-01.

QUESTION 14

Recent as of 2/2/2021

Why does CISA recommend users split out the web server from the Orion Application server?

By splitting out the web server from the application server, you can leverage different controls to further secure your deployment. Orion Platform users need access to the web server (port 443), which could have a large surface area, and the web server does *not* need to have network access to the monitored devices – only the pollers (including the main poller) need network access. By deploying a separate web server and shutting down and/or blocking access to the web console on the main poller, you can put a firebreak between the web interface used by users and the monitored systems.

QUESTION 15

Recent as of 1/13/2021

What is SolarWinds doing to help find a solution?

Since the cyberattack on our customers and SolarWinds, we've worked around the clock to support our customers. As we shared in our recent update, we're partnering with multiple industry-leading cybersecurity experts to strengthen our systems, further enhance our product development processes, and adapt the ways that we deliver powerful, affordable, and secure solutions to our customers. Read more on the latest findings from our investigation of SUNBURST here.

We have retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion Platform products was exploited as a point of any infiltration of customer systems, and in the development of appropriate mitigation and remediation plans. SolarWinds is cooperating and sharing information with partners, vendors, law enforcement, and the intelligence and government agencies around the world to assist in investigations related to this incident.

We are solely focused on our customers and the industry we serve. Our top priority has been to take all steps necessary to ensure that our and our customers' environments are secure. We are taking extraordinary measures to accomplish this goal. We shared all of our proprietary code libraries that we believed to have been affected by SUNBURST to give security professionals the information they needed to do their research. We also have had numerous conversations with security professionals to further assist them in their research. We were very pleased and proud to hear that colleagues in the industry discovered a "killswitch" that will prevent the malicious code from being used to create a compromise.

QUESTION 16

Recent as of 12/26/2020

What if I can't upgrade right now? How do I ensure the security of my Orion server?

If you can't upgrade immediately, please follow the guidelines available here for improving the security of your Orion Platform instance. Primary mitigation steps include:

- Ensure the Orion Platform is installed behind a firewall,
- Disable internet access for the Orion Platform, and
- Limit the ports and connections to only what is required to operate your platform.

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

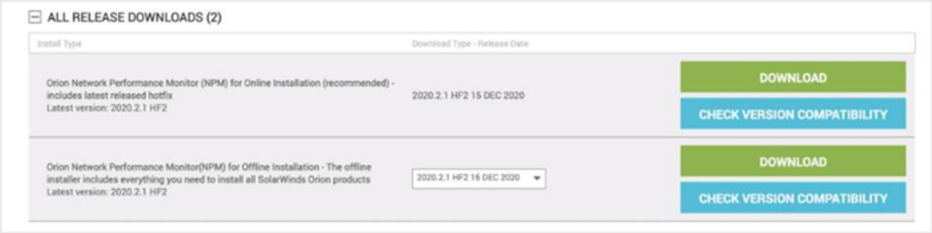
QUESTION 17

Recent as of 12/18/2020

I have downloaded a file from my Customer Portal and want to verify it is legitimate. How can I do that?

A list of SolarWinds Checksums is available here for your reference. If you're unaware of how to perform this validation, one such method is using "Get-FileHash" from the Microsoft PowerShell Utility documented here.

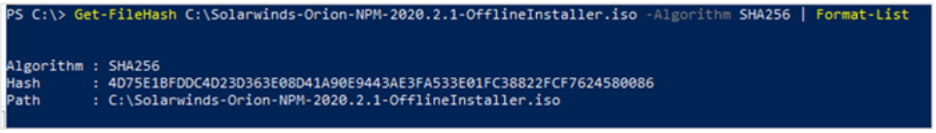
As an example, the Solarwinds-Orion-NPM-2020.2.1-OfflineInstaller.iso was obtained through the Customer Portal:



⊟ ALL RELEASE DOWNLOADS (2)

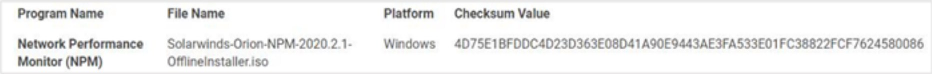
Install Type	Download Type - Release Date	
Orion Network Performance Monitor (NPM) for Online Installation (recommended) - includes latest released hotfix Latest version: 2020.2.1 HF2	2020.2.1 HF2 15 DEC 2020	DOWNLOAD CHECK VERSION COMPATIBILITY
Orion Network Performance Monitor(NPM) for Offline Installation - The offline installer includes everything you need to install all SolarWinds Orion products Latest version: 2020.2.1 HF2	2020.2.1 HF2 15 DEC 2020 ▾	DOWNLOAD CHECK VERSION COMPATIBILITY

Once downloaded, the steps to compute the hash value for an ISO file were followed from here. Here is an example output and matching checksum available below. Note: A response may take a few moments.



```
PS C:\> Get-FileHash C:\Solarwinds-Orion-NPM-2020.2.1-OfflineInstaller.iso -Algorithm SHA256 | Format-List


Algorithm : SHA256
Hash      : 4D75E1BFDDC4D23D363E08D41A90E9443AE3FA533E01FC38822FCF7624580086
Path      : C:\Solarwinds-Orion-NPM-2020.2.1-OfflineInstaller.iso
```



Program Name	File Name	Platform	Checksum Value
Network Performance Monitor (NPM)	Solarwinds-Orion-NPM-2020.2.1-OfflineInstaller.iso	Windows	4D75E1BFDDC4D23D363E08D41A90E9443AE3FA533E01FC38822FCF7624580086

QUESTION 18

Recent as of 4/6/2021

Where can I see a complete list of all Orion Platform versions, their status and recommended actions?

If you’re unable to upgrade at this time, we have provided a script that customers can install to temporarily protect their environment against SUPERNOVA***. The script is available at https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip. If you reinstall your Orion server, you will need to reapply this script.

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 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
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/Super**

*****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.

QUESTION 19

Recent as of 1/13/2021

If your environment was compromised, why is it safe for us to install these updates/trust your code? OR What are you doing to prevent future incidents moving forward?

Our investigations are ongoing, but since the vulnerabilities related to SUNBURST and SUPERNOVA were discovered, we have reviewed our environment, giving an initial focus on ensuring the security of our build environment, including our source code repositories. We have reviewed the architecture of the build environment, the privileged and non-privileged users that have access to the build environment, and the network surrounding the build environment.

We have retained third-party cybersecurity experts to assist in an investigation of these matters, including whether the vulnerabilities were exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans to help ensure future releases are protected. We are also cooperating and sharing information with our partners, vendors, and law enforcement, intelligence, and government agencies around the world to assist in investigations and to avoid vulnerabilities in future releases.

Our investigations are ongoing, and we will continue to focus on ensuring that our environments are secure and protected. Read more about our investigation here, and read more about the actions we're taking moving forward here.

QUESTION 20

Recent as of 12/15/2020

I still have more questions about this issue and my environment's security—who can I talk to?

We are making regular updates to our Security Advisory page at solarwinds.com/securityadvisory.

QUESTION 21

Recent as of 12/15/2020

Why can't you tell us more about what's going on?

While we understand there may a lot of questions on this situation, we will continue to communicate information as it's available. Our investigations into these matters are ongoing, and we continue to work closely with law enforcement, intelligence and other government agencies around the world to investigate them. We are also working with leading security experts in these investigations and to help further secure our products and internal systems.

QUESTION 22

Recent as of 2/5/2020

What about the vulnerabilities disclosed by Trustwave?

First, it's important to note these vulnerabilities are not related to the SUNBURST attack, or to SUPERNOVA.

Vulnerabilities of varying degrees are common in all software products, including recent patches for Apple and Microsoft that solve critical vulnerabilities, but we understand there is heightened scrutiny on SolarWinds right now. SolarWinds has always been committed to working with our customers and other organizations to identify and remediate any vulnerabilities across our product portfolio in a responsible way. Trustwave is a leading threat detection company that responsibly reports product vulnerabilities to companies as they are discovered prior to broader announcement to allow companies to develop remediations to protect their customers.

The vulnerabilities announced by Trustwave concerning the Orion® Platform were addressed in Orion Platform version 2020.2.4, released January 25, 2021. The vulnerabilities concerning Serv-U were addressed in Serv-U version 15.2.2 HF1, released January 22, 2021. To review the list of currently supported versions of these products, please review the documentation.

Trustwave identified three vulnerabilities, two in the Orion Platform and one in our Serv-U file transfer product. To our knowledge, none of these vulnerabilities have been exploited. The three vulnerabilities could be described as follows:

- The first, which affects the Orion Platform, allows for an unprivileged user to extract passwords from the SQL Server database.
- The second allows a remote user to execute a command against the Microsoft Message Queue service used by the Orion Platform.
- The third allows an attacker to gain access to the Serv-U FTP server by creating an unauthorized user account.

QUESTION 23

Recent as of 2/5/2020

What about the issue disclosed by Sophos?

In the case of the Sophos announcement, it is important to note this is **NOT** a reported vulnerability in the Orion Platform product. This situation was the result of a compromise within an individual company's network unrelated to SolarWinds. That breach enabled attackers to add malicious code to the Orion Platform software instance within the customer's network.

- In November of 2020, Sophos investigated an environment infected with a Ragnar Locker attack in which hundreds of computers were compromised.
- One of the computers compromised in the Ragnar Locker attack was a Windows server hosting the Orion product.
- The threat actor had full administrative access to the Windows server and was able to copy and replace a signed .dll shipped with the Orion Platform software with an unsigned, compromised version.
- This compromised code was not shipped with the Orion Platform software.
- Following the Orion Secure Configuration Guide mitigates the risk of this type of attack.

QUESTION 24

Recent as of 1/29/2021

What is SUPERNOVA?

Shortly after SUNBURST was announced, third parties and the media publicly reported on a malware, now referred to as SUPERNOVA. Based on our investigation, this malware could be deployed through an exploitation of a vulnerability in the Orion Platform. 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 before we disclose the vulnerabilities.

CISA released a malware analysis report on SUPERNOVA on January 27, 2021. 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 Orion Platform. The second is the exploitation of a vulnerability in the Orion Platform to enable deployment of the malicious code. The latest updates were designed to remediate this vulnerability in all supported versions of the Orion Platform.

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.

QUESTION 25

Recent as of 12/26/2020

Is SUPERNOVA another supply chain attack?

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.

QUESTION 26

Recent as of 12/29/2020

What indicators of compromise (IOCs) of the SUPERNOVA malware have you identified?

Through our investigations, our retention of a third-party cybersecurity firm, and in cooperation with the law enforcement, intelligence and other government agencies around the world in investigations related to the SUPERNOVA vulnerability, we’ve identified the following IOC:

- The SUPERNOVA malware [app_web_logoimagehandler.ashx.b6031896.dll] with the file hash:
- sha256 of the file app_web_logoimagehandler.ashx.b6031896.dll is: c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71

QUESTION 27

Recent as of 12/31/2020

How can I confirm if I’ve applied either the SUPERNOVA mitigation script or one of the SUPERNOVA security fixes to my Orion server(s)?

If you’re running Orion Platform version 2018.2, 2018.4, or 2019.2, you can run the script available here to verify one of the SUPERNOVA Security Fixes (2018.2 HF6 Security Fix, 2018.4 HF3 Security Fix, 2019.2 HF3 Security Fix) for the recent SUPERNOVA security vulnerability has been applied to your main Orion server and any additional web servers. If you reinstall your Orion server, you will need to reapply the respective patch.

If you used the SUPERNOVA Mitigation Script to address the Supernova vulnerability, use the guidance in the document within that package to confirm the temporary patch. If you reinstall your Orion server, you will need to reapply this script.

QUESTION 28

Recent as of 12/18/2020

What is SUNBURST?

SolarWinds was the victim of a cyberattack 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 Platform products run. SUNBURST was 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.

Based on our investigation, 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 sophistication and nature of SUNBURST indicates that it may have been conducted by an outside nation state, but SolarWinds has not verified the identity of the attacker.

QUESTION 29

Recent as of 12/18/2020

How extensive is the impact of SUNBURST?

Based on our investigations to date, which are ongoing, we believe that the SUNBURST vulnerability was inserted within the Orion Platform products and existed in updates released between March and June 2020 (which we call the "relevant period") as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion Platform products. SolarWinds has taken steps to remediate the compromise of the Orion software build system and we're investigating what additional steps, if any, should be taken. **Also, while we are still investigating our non-Orion products, we have not seen any evidence that they are impacted by SUNBURST.** Based on our investigations to date, SolarWinds currently believes that:

- Orion Platform products downloaded, implemented or updated during the relevant period contained the SUNBURST vulnerability;
- Orion Platform products downloaded and implemented **before** the relevant period and not updated during the relevant period did not contain the SUNBURST vulnerability;
- Orion Platform products downloaded and implemented **after** the relevant period did not contain the SUNBURST vulnerability; and
- Previously affected versions of the Orion Platform products that were updated with a build released **after** the relevant period no longer contained the SUNBURST vulnerability; however, the server on which the affected Orion Platform products ran may have been compromised during the period in which the SUNBURST vulnerability existed.

QUESTION 30

Recent as of 4/6/2021

What should I do if I believe my environment has been compromised by the SUNBURST vulnerability?

If you believe your environment has been compromised by the SUNBURST vulnerability, below are the recommended steps to take:

First, determine the version of the Orion® Platform products you have installed here, and verify which hotfix updates you have installed here.

- If you **have** already upgraded to **2020.2.5**, additional security fixes and protections unrelated to SUNBURST and SUPERNOVA are included in this version. For more information, review the Release Notes here, and KB article here.

- If you have upgraded to **2020.2.4** or **2019.4 HF 2**, both the SUNBURST and SUPERNOVA vulnerabilities have been addressed in these versions—and they have also been digitally re-signed by newly obtained digital code-signing certificates.

- If you **have not** already upgraded to **2020.2.5**, **2020.2.4**, or **2019.4.2**, follow the guidance identified for your current version of your Orion Platform products below to help ensure the security of your environment:

- If you're currently running Orion Platform version **2019.4 HF 4**, we recommend you upgrade to **2020.2.5**, or **2019.4.2** if you are unable to upgrade to the latest version at this time.
- If you're currently running Orion Platform version **2019.4 HF 5**, we recommend you rebuild your Orion server/VM for all pollers and install Orion Platform version **2020.2.5** or **2019.4.2** if you are unable to upgrade to the latest version at this time.
- If you're currently running Orion Platform version **2020.2.1**, **but have run any of the previous infected versions**, rebuild your Orion server and/or VM for all pollers and install Orion Platform version **2020.2.5** on a fresh machine.
- If you are running a version prior to Orion Platform version **2019.4 HF 4**, we do not believe that your system was compromised with this vulnerability. We still recommend as a best practice that you upgrade to the latest version, Orion Platform version **2020.2.5**, to take advantage of the latest security improvements.

To help protect your system, you should also block DNS access to any of the following:

- avsvmcloud[.]com
- panhardware[.]com
- databasegalore[.]com
- freescanonline[.]com
- thedoccloud[.]com
- deftsecurity[.]com

If you have the expertise to take the additional following action items, please do so:

- Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion Platform [versions **2019.4 HF 5**, **2020.2 unpatched**, and **2020.2 HF 1**].
- Analyze stored network traffic for indications of compromise, including new external DNS domains.
- Consult with any security vendors with whom you currently have a relationship on their recommendations.

QUESTION 31

Recent as of 4/6/2021

If my Orion server currently or previously had a SUNBURST vulnerable version, should I simply upgrade or should I rebuild my Orion server? What about my database?

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.

- If you **never ran** a known, affected version on your Orion server, **we do not recommend that you rebuild**. We still recommend as a best practice that you upgrade to the latest version, Orion Platform version **2020.2.5**,to take advantage of the latest security improvements.
- If you ran a known, affected version of your Orion server **and** it had access to the internet, we recommend that **you rebuild the server**.
- If your Orion server had no access to the internet, **we do not recommend that you rebuild**. An upgrade to Orion Platform version **2020.2.5** will be sufficient.

If you rebuild your servers, here are the factors to consider in deciding whether to retain your Orion Database:

- **Reference the CISA Alert (AA20-352A):**
  - If you fall into **Category 2**, you should be able to re-install the software and retain your Orion databases for the platform, for flow, and for logs—consistent with a thorough risk evaluation.
  - If you fall into **Category 3**, your Orion installation—including the Orion databases—are equally as vulnerable as the rest of the environment, and you should follow your incident response procedures.
- **Additional considerations:**
  - We are not aware of any indications at this time that the SUNBURST vulnerability routinely altered the Orion databases in any way.
  - You may want to audit configurations stored in the database, like alert actions, or executable scripts to confirm they have not been tampered with.
  - If you chose to rebuild your databases, follow your incident response procedures to image and retain your databases, particularly your flow database for forensic analysis.

QUESTION 32

Recent as of 12/16/2020

I want to manually check my version of the SolarWinds.Orion.Core.BusinessLayer.dll for the SUNBURST vulnerability. Do you know a way to do that?

You should check your Orion server, any additional polling engine, high availability (HA) engines, and additional web servers. You can use the following file hash information to check whether you have the version with the inserted vulnerability:

From Windows, open PowerShell and run the following (adjusting the file path if a different installation path was used):

```
Get-FileHash "C:\Program Files (x86)\SolarWinds\Orion\SolarWinds.Orion.Core.BusinessLayer.dll"
```

Versions not known to contain the SUNBURST vulnerability:

2020.2.1 RTM sha256sum of SolarWinds.Orion.Core.BusinessLayer.dll (file version 2020.2.15300.12766)

143632672dcb6ef324343739636b984f5c52ece0e078cfee7c6cac4a3545403a

(No hotfix applied, not the known compromised version)

2020.2.1 HF 1 sha256sum of SolarWinds.Orion.Core.BusinessLayer.dll (file version 2020.2.15300.12766)

143632672dcb6ef324343739636b984f5c52ece0e078cfee7c6cac4a3545403a

(Not the known compromised version; NOTE: same as 2020.2.1 RTM – this hotfix does not update that DLL)

2019.4 HF6 - file version 2019.4.5200.9106 - sha256 8DFE613B00D495FB8905BDF6E1317D3E3AC1F63A626032FA2BDAD4750887EE8A

2020.2.1 HF2 - file version 2020.2.15300.12901 - sha256
CC870C07EEB672AB33B6C2BE51B173AD5564AF5D98BFC02DA02367A9E349A76F

Versions known to contain the SUNBURST vulnerability:

sha256 of SolarWinds.Orion.Core.BusinessLayer.dll from 2019.4 HF 5:
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77

sha256 of SolarWinds.Orion.Core.BusinessLayer.dll from 2020.2:
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6

Hashes from fixes provided to individual customers, sometimes called “Buddy Drops”

019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134

ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c

c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77

dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b

eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed

Path: SolarWinds.Orion.Core.BusinessLayer.dll.

By default, the file is located in C:\Program Files (x86)\SolarWinds\Orion.

NOTE: If you’re checking files using MacOS or Linux, the standard “sha256sum” tool can be used.

QUESTION 33

Recent as of 12/15/2020

What indicators of compromise (IOCs) of the SUNBURST vulnerability have you identified?

Through our investigations, our retention of a third-party cybersecurity firm, and in cooperation with the law enforcement, intelligence, and other government agencies around the world in investigations related to the SUNBURST vulnerability, we’ve identified the following IOCs:

- [SolarWinds.Orion.Core.BusinessLayer.dll] with one of the file hashes listed below:
- sha256 of SolarWinds.Orion.Core.BusinessLayer.dll from 2019.4 HF 5:
  32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
- sha256 of SolarWinds.Orion.Core.BusinessLayer.dll from 2020.2:
  ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6

Additional Hashes from Hotfix and Buddy drop releases

- 019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
- ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
- c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
- dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
- eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed

QUESTION 34

Recent as of 12/20/2020

How do I know someone didn't exploit the SUNBURST vulnerability and move horizontally in my environment and compromise another system?

If the SUNBURST vulnerability was exploited in your environment, you may see network traffic from the Orion server to the internet. This traffic would be directed to a domain other than SolarWinds domain. Horizontal or lateral movement by an attacker would indicate that they have gained privileged level access to your environment. Increased security event monitoring, close inspection of server and application access logs, and understanding what local accounts exist on your corporate systems will help to identify any signs of misuse.

For further details, please see **CERT Alert (AA20-352A), Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations**, updated December 19, 2020: https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

QUESTION 35

Recent as of 12/24/2020

What products are affected by the SUNBURST vulnerability?

We have identified the following products as being affected: Orion Platform versions **2019.4 HF 5**, **2020.2 unpatched,** and **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)
Network Performance Monitor (NPM)
NetFlow Traffic Analyzer (NTA)
Server & Application Monitor (SAM)
Server Configuration Monitor (SCM)
Storage Resource Monitor (SRM)
User Device Tracker (UDT)
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.

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.

QUESTION 36

Recent as of 12/20/2020

What products are NOT affected by the SUNBURST vulnerability?

Our investigations are still ongoing, but based on our investigations to date, we have found no evidence that other versions of our Orion Platform products or any of our other products, Orion agents, or Web Performance Monitor (WPM) Players are affected by the SUNBURST vulnerability.

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

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

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

Engineer’s Toolset

Engineer's Web Toolset

FailOver Engine

Firewall Security Monitor

Identity Monitor

ipMonitor

Kiwi CatTools

Kiwi Syslog Server

LANSurveyor

Librato

Log & Event Manager (LEM)

Log and Event Manager Workstation Edition

Loggly

Mobile Admin

Network Topology Mapper (NTM)

Papertrail

Patch Manager

Pingdom

Pingdom Server Monitor

Security Event Manager(SEM)

Security Event Manager Workstation Edition

Server Profiler

SentryOne Test

Task Factory

DBA xPress

Plan Explorer

APS Sentry

DW Sentry

SQL Sentry Essentials

SentryOne Monitor

BI xPress

SolarWinds MSP Products:

N-central – Probe

N-central – Topology

N-central – NetPath

N-central

NetPath – Server

RMM

Backup Disaster Recovery

M365 Backup

Backup

Mail Assure

SpamExperts

MSP Manager

PassPortal

Take Control

Patch

Automation Manager

Webprotection

QUESTION 37

Recent as of 12/15/2020

Why didn’t SolarWinds catch the SUNBURST vulnerability before it happened?

This SUNBURST vulnerability was very complex and sophisticated. It was crafted to evade detection and only run when detection was unlikely.

QUESTION 38

Recent as of 12/15/2020

With these processes in place how was your code compromised to insert the SUNBURST vulnerability?

We are not aware that the SolarWinds code base was compromised. Our initial investigations point to an issue in the Orion software build system in which the SUNBURST vulnerability was inserted which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion Platform products run.

QUESTION 39

Recent as of 12/15/2020

How many customers are potentially affected by SUNBURST vulnerability?

We’ve currently identified less than 18,000 customers potentially affected by this security vulnerability.

QUESTION 40

Recent as of 12/15/2020

Why were 33,000 customers mentioned in connection with the SUNBURST vulnerability?

Out of an abundance of caution, we’ve communicated with all SolarWinds customers on active maintenance from February 2020 through current. We initially communicated with more customers than we believe were affected by the SUNBURST vulnerability, and this number was included in our Form 8-K filed with the Securities Exchange Commission on December 14, 2020.

QUESTION 41

Recent as of 2/4/2021

What is the Common Criteria framework?

Common Criteria is a framework most often associated with federal organizations. It’s an international standard for computer security achieved by national laboratory testing and evaluation. Please refer to this KB Article for more information on products included under the Orion Suite for Federal Government.

QUESTION 42

Recent as of 2/24/2021

Where can I see a complete list of Orion Suite for Federal Government versions, their status and recommended actions?

Current Version	Orion Platform Version	Action Required	Vulnerable to SUNBURST?	Vulnerable to SUPERNOVA?
Orion Suite v4.1	Orion Platform v2019.2 HF4	No Action Needed	NO	NO
Orion Suite v4.0	Orion Platform v2019.2 HF3	Apply SUPERNOVA Security Patch on top of 2019.2 HF 3 or upgrade to 2019.2 HF 4	NO	YES
Orion Suite v3.0	Orion Platform v2017.3.5 SP 5	Apply SUPERNOVA mitigation script or upgrade to 2019.2 HF 4	NO	YES
Orion Suite v2.0	Orion Platform V2015.1.2	Apply SUPERNOVA mitigation script or upgrade to 2019.2 HF 4	NO	YES
Orion Suite v1.0	No documented Orion Platform version – NPM V10.6.0 / SAM V6.0.0	Apply SUPERNOVA mitigation script or upgrade to 2019.2 HF 4	NO	YES