# FINISHED INTELLIGENCE REPORTS

## SUPERNOVA Malware Analysis Report


TLP:WHITE

Jan 27, 2021

On January 27, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued a Malware Analysis Report (MAR), MAR-10319053-1.v1, on several malicious artifacts affecting the SolarWinds Orion product identified by the security company FireEye as SUPERNOVA.

According to a SolarWinds advisory, SUPERNOVA is not embedded within the Orion platform as a supply chain attack and is instead placed by an attacker directly on a system that hosts SolarWinds Orion and is designed to appear as part of the SolarWinds product. CISA's assessment is that SUPERNOVA is not part of the SolarWinds supply chain attack previously described in CISA (AA20-352A) alert.

The full CISA (AA21-027a) Malware Analysis Report is available for your review.

This report describes the analysis of a PowerShell script that decodes and installs SUPERNOVA, a malicious webshell backdoor. SUPERNOVA is embedded in a trojanized version of the Solarwinds Orion Web Application module called "App_Web_logoimagehandler.ashx.b6031896.dll." The SUPERNOVA malware allows a remote operator to dynamically inject C# source code into a web portal provided via the SolarWinds software suite. The injected code is compiled and directly executed in memory.

- 290951fcc76b497f13dcb756883be3377cd3a4692e51350c92cac157fc87e515 (1.ps1)
    - This file is an event log that details the execution of a PowerShell script designed to Base64 decode and install a 32-bit .NET dynamic-link library (DLL) into the following location: "C:\inetpub\SolarWinds\bin\App_Web_logoimagehandler.ashx.b6031896.dll (c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71). The DLL is patched with the SUPERNOVA webshell and is a replacement for a legitimate SolarWinds DLL.
- c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71 (App_Web_logoimagehandler.ashx.b6031896.dll)
    - This file is a 32-bit .NET DLL that has been identified as a modified SolarWinds plug-in. The malware patched into this plug-in has been identified as SUPERNOVA. The modification includes the "DynamicRun" export function which is designed to accept and parse provided arguments. The arguments are expected to partially contain C# code, which the function will compile and execute directly in system memory. The purpose of this malware indicates the attacker has identified a vulnerability allowing the ability to dynamically provide a custom "HttpContext" data structure to the web application's "ProcessRequest" function.
- 02c5a4770ee759593ec2d2ca54373b63dea5ff94da2e8b4c733f132c00fc7ea1 (AssemblyInfo__.ini)
    - --Begin text--
      App_Web_logoimagehandler.ashx.b6031896,0.0.0.0,, file:///C:/InetPub/SolarWinds/bin/App_Web_logoimagehandler.ashx.b6031896.dll
      --End text--

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, "Guide to Malware Incident Prevention & Handling for Desktops and Laptops".

| | |
|---|---|
| **Reference(s)** | cisa, NIST-NVD |
| **Report Source(s)** | CISA |

## Recommendations

- CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.
- Maintain up-to-date antivirus signatures and engines.

- Keep operating system patches
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.

- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).

- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

**Release Date**
Jan 27, 2021

**Sources**

MAR-10319053-1.v1 - Supernova

(NIST) Special Publication 800-83, "Guide to Malware Incident Prevention & Handling for Desktops and Laptops"

**Alert ID** 06cac53d

## View Alert

**Tags** SUPERNOVA, SolarWinds

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**For Questions or Comments** Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**