

# CERT/CC Vulnerability Note VU#843464

Archived: 2026-04-06 00:05:05 UTC

## Overview

The SolarWinds Orion API is vulnerable to authentication bypass that could allow a remote attacker to execute API commands.

## Description

The [SolarWinds Orion Platform](#) is a suite of infrastructure and system monitoring and management products. The [SolarWinds Orion API](#) is embedded into the Orion Core and is used to interface with all SolarWinds Orion Platform products. API authentication can be bypassed by including specific parameters in the [Request.PathInfo](#) portion of a URI request, which could allow an attacker to execute unauthenticated API commands. In particular, if an attacker appends a `PathInfo` parameter of `WebResource.axd`, `ScriptResource.axd`, `i18n.ashx`, or `Skipi18n` to a request to a SolarWinds Orion server, SolarWinds may set the [SkipAuthorization](#) flag, which may allow the API request to be processed without requiring authentication.

This vulnerability, also known as CVE-2020-10148, is the vulnerability that SolarWinds has [indicated](#) to have been used to install the malware known as SUPERNOVA.

We have created a python3 script to check for vulnerable SolarWinds Orion servers: [swcheck.py](#)

## Impact

This vulnerability could allow a remote attacker to bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance.

## Solution

### Apply an Update

Users should update to the relevant versions of the SolarWinds Orion Platform:

- 2019.4 HF 6 (released December 14, 2020)
- 2020.2.1 HF 2 (released December 15, 2020)
- 2019.2 SUPERNOVA Patch (released December 23, 2020)
- 2018.4 SUPERNOVA Patch (released December 23, 2020)
- 2018.2 SUPERNOVA Patch (released December 23, 2020)

More information can be found in the [SolarWinds Security Advisory](#).

### Harden the IIS Server

Especially in cases when updates cannot be installed, we recommend that users implement [these mitigations](#) to harden the IIS server.

## Acknowledgements

This document was written by Madison Oliver and Will Dormann.

## Vendor Information

843464

Filter by status:

Filter by content: Additional information available

Sort by:

## References

- <https://www.solarwinds.com/securityadvisory>
- <https://cyber.dhs.gov/ed/21-01/>
- <https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software>
- <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a>
- <https://github.com/solarwinds/OrionSDK/wiki>
- <https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip>

## Other Information

<b>CVE IDs:</b>	<a href="#">CVE-2020-10148</a>
<b>Date Public:</b>	2020-12-26
<b>Date First Published:</b>	2020-12-26
<b>Date Last Updated:</b>	2021-01-28 16:53 UTC
<b>Document Revision:</b>	12

---

Source: <https://www.kb.cert.org/vuls/id/843464>