SingCERT
Singapore Computer Emergency Response Team

Remote Command Execution Vulnerability in SolarWinds Orion Platform

Published on 28 Dec 2020

Updated on 28 Dec 2020

SolarWinds has released an updated security advisory to include information on the SUPERNOVA malware which was found to be exploited through a vulnerability (CVE-2020-10148) in the Orion Platform.

Successful exploitation of the vulnerability could allow attackers to remotely bypass authentication and execute API commands which may result in a compromise of the SolarWinds instance.

Administrators are advised to update to the following relevant versions of the SolarWinds Orion Platform as soon as possible:

- 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)

For administrators who have already upgraded to 2020.2.1 HF 2 or 2019.4 HF 6 versions, no further action is required.

Affected administrators who are unable to install the security updates immediately are advised to temporarily protect their environment by applying mitigating measures recommended by SolarWinds.

Instructions on the measures can be found here:

https://downloads.solarwinds.com/solarwinds/Support/SupernovaMitigation.zip

More information is available here:

https://kb.cert.org/vuls/id/843464 https://www.solarwinds.com/securityadvisory

https://www.csa.gov.sg/singcert/alerts/al-2020-049

Last Updated 28 Dec 2020