National Cyber Security Centre

2012281112-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Flash Alert

SolarWinds Orion RCE Vulnerability (SUPERNOVA)
2020-12-28

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type	The NCSC has received information that the SolarWinds Orion API is vulnerable to authentication bypass that could allow a remote attacker to execute API commands. SolarWinds have provided the below information on SUPERNOVA: • SUPERNOVA is not malicious code embedded within the builds of the Orion Platform as a supply chain attack. It is malware that is separately placed on a server that requires unauthorised 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. • The full SolarWinds advisory can be found here.
Products Affected	All Orion Platform products, except those customers already on **Orion Platform versions 2019.4 HF 6** or **2020.2.1 HF 2**.
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.
Recommendations	Orion Platform versions 2019.4 HF6 and 2020.2.1 HF2 were designed to protect from both SUNBURST and SUPERNOVA. If you are using one of those versions, we do not recommend that you take any actions at this time. We recommend that all active maintenance customers of Orion Platform products, except those customers already on Orion Platform versions 2019.4 HF 6 or 2020.2.1 HF 2, apply the latest updates related to the version of the product they have deployed, as soon as possible. These updates contain security enhancements including those designed to protect you from SUNBURST (See our previous advisory here) and SUPERNOVA. **NOTE:** If you reinstall, you need to re-apply the patch or hotfix. If you're unable to upgrade at this time, SolarWinds have provided a script that customers can install to temporarily protect their environment against the SUPERNOVA malware. The script is available here.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie