National Cyber Security Centre

2012151105-NCSC

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

NCSC Flash Alert

SolarWinds Software Exploited (SUNBURST)
UPDATE - 2020-12-16

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 advanced threat actors are actively exploiting SolarWinds Orion Platform software versions 2019.4 through 2020.2.1, released between March 2020 and June 2020. Please review the SolarWinds advisory here. This supply chain attack affecting SolarWinds Orion is being used to distribute malware labelled as SUNBURST. The threat actors have taken multiple steps to hide and obfuscate activity and have shown a high level of operational security (OPSEC) and sophistication. NCSC-IE recommends that affected organisations review the Recommendations section below and to **upgrade to Orion Platform version 2020.2.1 HF 2 as a matter of urgency**.
Products Affected	SolarWinds Orion Platform software version builds for versions *2019.4 HF 5*, *2020.2 with no hotfix installed* and *2020.2 HF 1*.
Impact	Compromised Information Systems.
Recommendations	NCSC-IE recommends that affected organisations upgrade to **Platform version 2020.2.1 HF 2** as soon as possible, to ensure the security of your environment. The **2020.2.1 HF 2** release both replaces the compromised component and provides several additional security enhancements. The latest version is available in the SolarWinds Customer Portal. SolarWinds also advise that organisations with any of the products for Orion Platform v2019.4 HF 5 listed here to update to 2019.4 HF 6. If you are not sure which version of the Orion Platform you are using, see directions on how to check that here. To check which hotfixes you have applied, please go here. NCSC-IE also recommends affected organisations follow these steps: • Ensure that all SolarWinds Orion Servers are isolated and all relevant patches and hotfixes are applied. • Check web proxy, DNS proxy and firewall logs for *avsvmcloud[.]com*. The malware attempts to resolve a subdomain of *avsvmcloud[.]com* and the DNS response will then deliver a CNAME record that directs to a command and control (C&C) domain. • Change all passwords on accounts associated with instances of Orion Server. • Review FireEye's GitHub page for countermeasures and IoC's. Use the signatures provided by FireEye to identify related activity. • Where resources and business continuity constraints permit, organisations should consider a full system rebuild of affected SolarWinds host systems.

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