U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00079

SOLARWINDS ORION ACTIVE EXPLOIT

DATE ISSUED: 15th December 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

A critical vulnerability in the SolarWinds Orion network management platform, versions 2019.4 -2020.2.1, are under known exploitation by a sophisticated threat actor according to CERT NZ and other sources. Initial indications suggest that the same threat actor responsible for the FireEye attack is the culprit for the SolarWinds Orion compromise.

BREAKDOWN

If exploited, this vulnerability introduces a backdoor to any server running the SolarWinds Orion platform, potentially allowing Remote Code Execution (RCE) to compromise networks and exfiltrate data. A number of other products may be potentially effected and a full list can be found using the sources listed below. Whilst so far, reports of compromise are coming from the United States, and only a small percentage of SolarWinds customers have been effected, any server housing this platform is potentially exposed and vulnerable to attack. This highly targeted and sophisticated attack is linked through supply chain to the FireEye incident reported last week and show similar characteristics in the level of sophistication, knowledge of operational security and avoidance techniques. Initially, SUNBURST malware was deployed using a fake update for the SolarWinds platform.

REMEDIATION STEPS

- Implement the hotfix provided by SolarWinds
- Consider isolating servers running SolarWinds Orion network management software to remove internet egress traffic until patches can be applied
- Change passwords to any accounts accessible to Orion servers and check server configurations

REFERENCES & RESOURCES

CERT NZ:	https://www.cert.govt.nz/it-specialists/advisories/solarwinds-orion-vulnerability-being-actively-exploited/
SolarWinds Security:	https://www.solarwinds.com/securityadvisory#https://www.solarwinds.com/securityadvisory
ZDNet:	https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/
	https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/