protiviti®
Face the Future with Confidence

CISA Issues Emergency Directive to Mitigate SolarWinds Orion Code Compromise

14 December
2020

On 13 December 2020, the Cybersecurity & Infrastructure Security Agency (CISA) issued an emergency directive detailing required action for federal agencies to mitigate the threat of the recently discovered compromise involving SolarWinds® Orion® Network Management products that are currently being exploited by malicious actors. (Read the SolarWinds Security Advisory here.) Given the nature of the threat and its potential impact on many industries outside of federal agencies and the public sector, organisations should take proactive steps to determine if this software revision is in use within their environment, and also evaluate their incident response function to ensure an appropriate level of vigilance.

The goal of an attacker attempting to capitalise on this code compromise is to gain initial access to an organisation's systems and maintain that unauthorised access despite typical interruptions to that initial foothold, like changes to access credentials and system restarts.

As more information is released, including patch fixes by SolarWinds, organisations with the SolarWinds Orion platform should consider proactive steps to reduce their exposure to this event:

- **Patch** – SolarWinds has released a Hotfix for this code compromise, with another expected on 15/12/2020. Organisations should continue to monitor guidance from SolarWinds as it releases more information.
- **Detection Opportunity** – Indicators of Compromise (IOC) have been released, as there are reports of active campaigns targeting private and public organisations. Organisations should use these IOCs to update their antivirus and endpoint detection and response (EDR) and scan their assets for anomalies that match the behaviour of this exploit. In addition, with the known IP addresses being used for this attack, organisations can block assets from communicating with domains behind these IP addresses.
- **Tabletop Analysis** – For organisations seeking additional guidance, the MITRE ATT&CK knowledge base lays out a good approach to examine the lifecycle, tools and

techniques associated with these types of exploit. Incident management teams should use the MITRE ATT&CK framework to understand the level of protection their organisation has at the various stages of this attack. This is a useful exercise to uncover blind spots that may need to be addressed. For example, the organisation may not have a system or tool to detect lateral movement, which is a technique an attacker would use to move through an organisation's environment after initial access via this code compromise.

- **Identity and Access Management Review** – An attacker exploiting this vulnerability is trying to gain initial access, evade detection and move laterally to identify a target or payload of interest. An attacker's ability to accomplish this goal or to dwell in an environment undetected is critically impacted by the strength of the organisation's identity and access management (IAM). Elements like privileged access management (PAM), identity federation, session management, services account management, and other core disciplines within an IAM program all play a crucial role in defending the organisation against these events. This is a good time to evaluate the organisation's IAM program and ensure adequate defense in depth against this and similar attack vectors.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000 and 35% of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti Can Help

Protiviti can assist companies with preparing for and responding to the evolving threats posed by ransomware and other cyberattacks. Contact Protiviti's Incident Response Team at IR@protiviti.com for technical, crisis management and investigative support.

protiviti®