Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Analyst Note

October 25, 2023 TLP:CLEAR Report: 202310251500

SolarWinds Critical Remote Code Execution Flaws

Executive Summary

SolarWinds has published security fixes for their Access Rights Manager (ARM). This update addressed eight vulnerabilities, with three of them being rated as critical (CVE-2023-35182, CVE-2023-35185, CVE-2023-35187) and can lead to remote code execution on the “SYSTEM” of a Windows computer. This could enable an attacker to operate with the highest level of privileges available on the machine. In early 2020, the SolarWinds Orion system was targeted by an attacker(s), which led to the supply chain compromise of up to 18,000 of its customers. Due to the previous malicious targeting and wide use of SolarWinds, HC3 strongly encourages users to monitor and upgrade their systems to prevent serious damage from occurring to the Healthcare and Public Health (HPH) sector.

Report

On October 18, 2023, SolarWinds published security fixes for their ARM software, which is a product that is designed to help security administrators provision, deprovision, manage, and audit user access rights to systems, data, and files. This can help IT infrastructure monitor for suspicious account activity. The Zero Day Initiative has identified eight vulnerabilities, with three of them being rated as critical. The critical flaws can allow for remote attackers to execute arbitrary code on the affected installation. Additional, authentication is not required for the exploitation of any of the three vulnerabilities and they can be leveraged in the context of “SYSTEM”. This could enable an attacker to operate with the highest level of privileges available on the machine and grant the attacker full control over files. Additional details on the vulnerabilities from the Zero Day Initiative are listed below:

- CVE-2023-35182: This flaw exists within the “createGlobalServerChannelInternal” method, which results from the lack of proper validation of user-supplied data that can result in a deserialization of untrusted data and can allow remote attackers to execute arbitrary code.
- CVE-2023-35185: This flaw exists within the “OpenFile” method, which results from the lack of proper validation of a user-supplied path prior to using it in file operations, and can allow remote attackers to perform directory traversal, which can lead remote code execution.
- CVE-2023-35187: This flaw exists within the “OpenClientUpdateFile” method, which results from the lack of proper validation of a user-supplied path prior to using it in file operations, and can allow remote attackers to execute arbitrary code.

SolarWinds Supply Chain Compromise

In early 2020, a global campaign occurred that targeted the public and private sector by conducting a supply chain attack through the SolarWinds Orion IT monitoring software. The campaign was tracked by Mandiant as UNC2452 and is believed to have been operated by APT29, a sophisticated Russian, state-sponored actor. APT29 has been conducting operations since at least 2008, and typically targets government networks in NATO member countries, along with a wide range of industries (see **Figure 1** below).

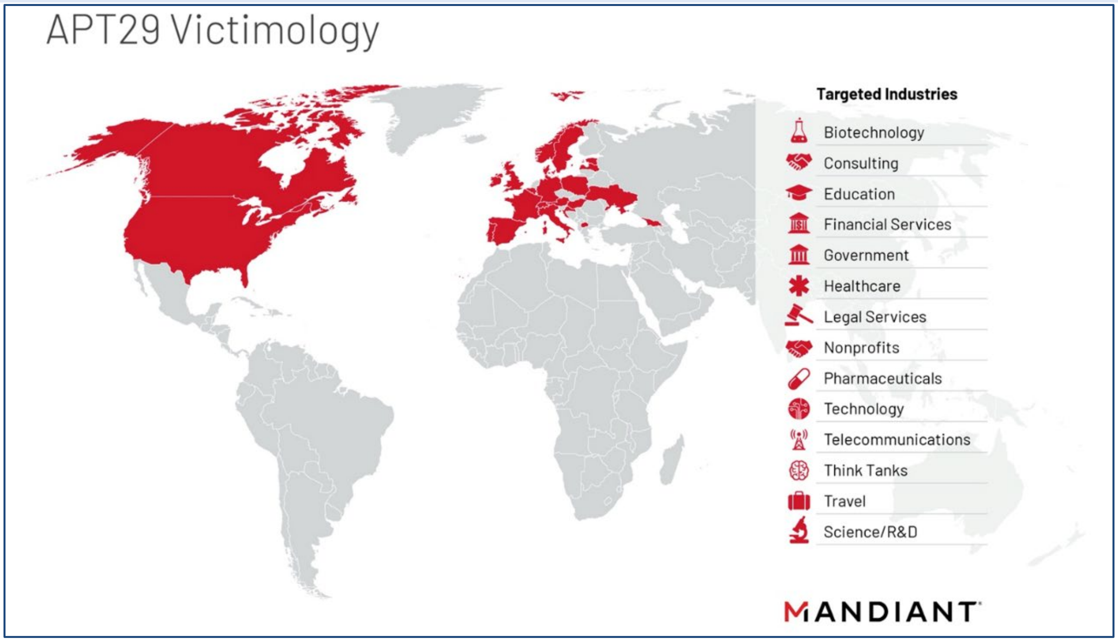

Figure 1: APT29 Victimology *(Source: Mandiant)*

During the compromise on SolarWinds in 2020, the Orion platform was targeted, which led to the distribution of the SUNBURST malware. This malware was a trojanized version of a digitally signed component from SolarWinds called “SolarWinds.Orion.Core.BusinessLayer.dll”. The plugin contained a backdoor that communicated through HTTP to third-party servers. The malware had a dormant period of up to two weeks, after which it would perform commands to transfer and execute files, profile the system, disable system services, and reboot, while attempting to blend in with legitimate traffic in the environment.

Supply chain attacks have the potential to cause serious damage after their initial compromise, because these malicious updates can be pushed downstream from a trusted source to many customers. Due to the popular use of the Orion platform, the attacker was reportedly able to compromise up to 18,000 SolarWinds customers, which included federal networks and the healthcare sector.

Impact to the HPH Sector

SolarWinds ARM software is used across a wide range of industries, including the HPH sector, as an internal tool to help IT security and administrators monitor account activity. The software is also used for managing user rights and access to data, which can be used to aid compliance with HIPAA security rules.

Patches, Mitigations, and Workarounds

HC3 encourages all users to adhere to manufactor’s guidance and upgrade their systems to the most current version, to prevent damage against the HPH sector. A complete list of the critical and high-severity vulnerabilities that were identified within the ARM software can be viewed here.

- ARM Installation and Upgrade Guide

Related Reports

- https://www.hhs.gov/sites/default/files/new-phishing-campaign-launched-solarwinds-attackers-sector-alert-tlp-white.pdf

References

Toulas, Bill. Critical RCE flaws found in SolarWinds access audit solution. Bleeping Computer. October 20, 2023. https://www.bleepingcomputer.com/news/security/critical-rce-flaws-found-in-solarwinds-access-audit-solution/

ZDI. SolarWinds Access Rights Manager createGlobalServerChannelInternal Deserialization of Untrusted Data Remote Code Execution Vulnerability. October 19, 2023. https://www.zerodayinitiative.com/advisories/ZDI-23-1564/

ZDI. SolarWinds Access Rights Manager OpenFile Directory Traversal Remote Code Execution Vulnerability. October 19, 2023. https://www.zerodayinitiative.com/advisories/ZDI-23-1565/

ZDI. SolarWinds Access Rights Manager OpenClientUpdateFile Directory Traversal Remote Code Execution Vulnerability. October 19, 2023. https://www.zerodayinitiative.com/advisories/ZDI-23-1567/

SolarWinds. ARM 2023.2.1 Release Notes. October 18, 2023. ARM 2023.2.1 Release Notes (solarwinds.com)

SolarWinds. ARM Installation and Upgrade Guide. https://documentation.solarwinds.com/en/success_center/arm/content/arm_installation_guide.htm

Mandiant. Assembling the Russian Nesting Doll: UNC2452 Merged into APT29. August 10, 2023. https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback