CYBR-445
Capstone Project
Fall 2023
SolarWinds Orion Report

Nycahri Griffin and Charlie White

Executive Summary

The Solarwinds Orion Platform is an environment that connects multiple Solarwinds products for network management and monitoring. The ease of having a single environment that can manage the whole network has made Solarwinds Orion Platform popular among government agencies and large corporations. In early 2020, the threat actor(s) successfully injected malicious code into an Orion software update. When remotely accessing the Orion management interface for a network, this code allowed a threat actor to bypass authentication and retrieve data from the network. Lion's Den on-prem Solarwinds Orion NMS has been identified as a victim of this attack.

Rated a critical vulnerability by the US National Institute of Standards and Technology (NIST), the recommended way to remedy this vulnerability is to update systems using Solarwinds Orion. Prevention of exploitation can be done by implementing patch testing and network segmentation. Proactively patching the systems and protecting against a vulnerability that many other companies have fallen victim to would display a dedication to security and work to reassure investors.

Background

SolarWinds Corporation is a company that develops and sells software to support businesses' IT infrastructure. They primarily develop network monitoring software (NMS), such as their products Loggly and Pingdom. SolarWinds' Orion Platform combines network management and network monitoring software that can be controlled from a consolidated environment. The Orion Platform's tools include a virtualization manager, server configuration monitor, user device tracker, network configuration manager, and Netflow traffic analyzer. The purpose of selling 12 tools in a single environment is for ease of access and assurance that all NMS are compatible. This made it popular with large companies and government entities. A few companies that deployed the United States Department of Veterans renewed their order in 2019, reported to cost $2.8 million, and many other US government departments have also been deploying SolarWinds NMS.

In September 2019, a threat actor began launching attacks on SolarWinds networks and testing code injection methods. They used test code to see if it was pushed out with Solarwinds product updates. Starting in early 2020, the threat actor began injecting malicious code into Solarwinds Orion software updates. The malicious code the threat actor injected can be used to create a backdoor into the SolarWinds Orion environment. This vulnerability was labeled CVE-2020-10148 with a rating of 9.8/10 (critical).

Methodology

The way the threat actors injected the malicious code into the software update is not publicly published, but its purpose is clear. When accessing the remote management user interface, the injected code allows users to bypass authentication by adding specific parameters to the URI request. With these parameters, the threat actor can access the SolarWinds Orion software and run API commands. A common Solarwinds API command is GET, which allows data retrieval from endpoints in the API.

Findings

The indicators of compromise (IoC) for CVE-2020-10148 are infected code and unusual network traffic. Check the version number to find if a system's Solarwinds Orion software contains infected code. Versions 2019.4 HF 5, 2020.2, and 2020.2 HF 1 are known to be infected. Another IoC would be unusual network traffic of access to the SolarWinds API and unusual requests to endpoints from the SolarWinds Orion system.

.

Impacts

This vulnerability impacts the business, whether it is exploited or not. A critical vulnerability like CVE-2020-10148 discourages investors from supporting Lion's Den and can be used against the company in court as proof of security negligence. The exploitation of CVE-2020-10148 against Lion's Den's network would mean a breach of the network perimeter and unauthorized access to data. A portion of this data is classified as personally identifiable information (PII) and must be protected in accordance with government regulations. Failing to do so would give agencies like the US Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC) grounds for legal action. The following downtime, investigations, possible private lawsuits, and cost of remedies would cost Lion's Den time and money. IBM reported that the global average data breach cost in 2023 was 4.45 million USD. A data breach can damage a company's credibility and trustworthiness, negatively affecting business traffic.

Recommendations

Recommendation 1:

Implement patch testing procedures to verify third-party software updates introduced to the Lion's Den's servers are secure and will not cause adverse effects to the organization's security posture.

Reasoning: Patch testing involves testing system or software patches in a controlled environment before deploying them within a system. Implementing patch testing would be a best practice procedure that relates to zero trust security, in which you trust nothing and verify everything. In Lion's Den case, patches and software updates from third-party providers (i.e., SolarWinds) should be tested in a controlled environment to assess how patches may affect the network, system, internal assets, etc. In doing so, Lion's Den's security posture is improved.

Recommendation 2:

Regularly apply patches to the system to address vulnerabilities.

Reasoning: Applying updates is a simple and relatively easy practice for protecting a system, yet it is often overlooked. Applying updates should be a practice at any size organization to patch known vulnerabilities, which will harden your system. We highly recommend that Lion's Den have standards and policies to identify and address vulnerabilities regularly. Running vulnerability scans will identify the vulnerabilities, and many scanners will provide solutions. This practice will protect Lion's Den's assets and reduce the network's attack surface.

Recommendation 3:

Implement network segmentation within the internal network.

Reasoning: Lion's Den's internal network consists of numerous servers with different functions; these servers should be segmented and isolated to protect from lateral movements if one server is compromised. In this case, the SolarWinds vulnerability would compromise the system and have virtually free range to explore other areas of the network. By implementing network segmentation, the vulnerability present in the SolarWinds server would be better contained.

Sources

"API methods." *SolarWinds*, 2023, https://documentation.solarwinds.com/en/success_center/sam/content/sam-api-poller-methods.htm. Accessed 5 Dec. 2023.

"Cost of a Data Breach Report 2023." *IBM*, https://www.ibm.com/reports/data-breach. Accessed 5 Dec. 2023.

"CVE-2020-10148." *NIST*, 3 Nov. 2021, https://nvd.nist.gov/vuln/detail/CVE-2020-10148. Accessed 5 Dec. 2023.

Jankowicz, Mia and Charles R. Davis. "These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia." *Business Insider*, 15 Dec. 2020, https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12. Accessed 5 Dec. 2023.

"SolarWinds." *Wikipedia*, 1 Nov. 2023, https://en.wikipedia.org/wiki/SolarWinds#2019%E2%80%932020_supply_chain_attacks. Accessed 5 Dec. 2023.

"SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)." *U.S. Government Accountability Office*, 22 April 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic. Accessed 5 Dec. 2023.

"SolarWinds Orion API authentication bypass allows remote command execution." *Carnegie Mellon University Software Engineering Institute*, 26 Dec. 2020.

"SolarWinds Security Advisory." *SolarWinds*, 6 April 2021, https://www.solarwinds.com/sa-overview/securityadvisory. Accessed 5 Dec. 2023.

"VA Implements SolarWinds to Enhance Visibility and Application Performance." *SolarWinds*, 2019, https://www.solarwinds.com/assets/solarwinds/swresources/case-study/fed-veteran-affairs-case-study.pdf?rev=cb87247b44ba4494b45f5306a5dc4e07&hash=278E640069D4A97DEA82F80F6A165F25. Accessed 5 Dec. 2023.

"2020 United States federal government data breach." *Wikipedia*, 18 Sep. 2023, https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach. Accessed 5 Dec. 2023.