FINISHED INTELLIGENCE REPORTS

Strategic Threat Intelligence: Preparing for the Next “SolarWinds” Event

TLP:WHITE

Apr 12, 2021

Health-ISAC, in cooperation with the American Hospital Association, has published our **Strategic Threat Intelligence: Preparing for the Next "SolarWinds" Event** report, which focuses on the key characteristics contributing to many enterprise network compromises, including the recent SolarWinds Orion incident.

The paper is meant for all audiences, non-technical and technical, as it presents strategic level decision elements that senior leaders including C-Suite Executives can use to help understand the risks involved with certain enterprise IT systems in their network environment. The intelligence also provides detailed technical analysis and recommendations for IT and information security teams

to help address immediate concerns by providing tactical mitigations and recommendations. For our technical audience, this paper presents a detailed analysis of characteristics that allowed the SolarWinds incident to affect multiple industries, organizations, and systems.

The ability to extract the characteristics and features of SolarWinds could allow organizations to predict and hopefully prevent the next "SolarWinds"-like event in their enterprise environments.

Key topics from the report include:

- Executive Summary
- SolarWinds - Characteristics that made the attack possible
- Other examples from the past
  - HP OpenView (2009)
  - Wannacry (2017)
  - Petya and NotPetya (2017)
  - SAP Solution Manager (SolMan) (2021)
- Technical Recommendations
- Recommendations from Health-ISAC and AHA
- Resources

Please see the attached research paper here. You may also access the content by navigating to the Doc Library in our Cyware Portal under Archives > Research Papers > H-ISAC AHA White Paper The Next SolarWinds.pdf

Reference(s)	Bleeping Computer, GitHub, cisa, Core Security, DHS, NIST-NVD, Network World, phe, Microsoft, Health-ISAC, cisa, ZDNet

Release Date
Apr 09, 2021

Sources
NIST: CVE-2003-0746: Various Distributed Computing Environment (DCE) for HP OpenView

Network World: HP Patches OpenView Vulnerabilities

Health-ISAC: SAP Solution Manager Flaw Weaponized with Proof of Concept Available

Core Security: HP OpenView Buffer Overflows Advisory ID Internal CORE-2009-0122

ZDNet: Microsoft: Petya Ransomware Attacks Were Spread by Hacked Software Updater

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Microsoft Shares CodeQL Queries to Scan Code for SolarWinds-Like Implants

SolarGate CodeQl Queries Github

Microsoft Blog: Turning the Page on Solorigate and Opening the Next Chapter for the Security Community

CISA Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products

DHS Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise

Alert ID be20ce1e

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat

visibility, new notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.