VULNERABILITY BULLETINS

CHIRP IOC Detection Tool Helps Detect Post-Supply Chain Compromise Threat Activity

○○○ TLP:WHITE

Mar 19, 2021

On March 18, 2021, CISA released Alert (AA21-077A) Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool.

Similar to Sparrow which scans for signs of APT compromise within an M365 or Azure environment, CHIRP scans for signs of APT compromise within an on-premises environment.

The CISA Hunt and Incident Response Program (CHIRP) provides forensic collection capability assistance to network defenders seeking to detect activity related to the supply chain compromises affecting SolarWinds and Active Directory/Microsoft 365.

The CISA Hunt and Incident Response Program (CHIRP) is a tool created to dynamically query Indicators of Compromise (IoCs) on hosts with a single package, outputting data in a JSON format for further analysis in a SIEM or other tool. CHIRP does not modify any system data.

The initial IoCs are intended to search for activity detailed in CISA Alert AA21-008A that has spilled into the enterprise environment.

Use CHIRP in your organization to:

- Examine Windows event logs for artifacts associated with this activity.
- Examine Windows Registry for evidence of intrusion.
- Query Windows network artifacts.
- Apply YARA rules to detect malware, backdoors, or implants.

Tools:

The CHIRP Tool is available from CISA’s Github repository. For additional guidance watch CISA's CHIRP Overview video.

Note: CISA will continue to release plugins and IOC packages for new threats via the CISA GitHub Repository.

Reference(s)	youtube, cisa, GitHub, cisa, fedscoop, Health IT Security, Bleeping Computer
Report Source(s)	CISA

Sources

Bleeping Computer - CISA Releases New SolarWinds Malicious Activity Detection ToolCISA - Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool

CISA - Github

FedScoop - CISA Shifting Focus to Monitoring the Insides of Networks for Cyberthreats

HealthITSecurity - DHS CISA Shares Incident Response Tool for On-Prem Threat Activity

Alert ID 284a202b

View Alert

Tags CHIRP, Sparrow, CISA, Azure

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

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**.