IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Ransomware Vulnerability Warning Pilot (RVWP)

March 2023

OVERVIEW

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents. Many of these incidents are perpetrated by ransomware threat actors using known vulnerabilities. By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experiencing a ransomware event. In addition, organizations should implement other security controls as described on stopransomware.gov.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which President Biden signed into law in March 2022, required CISA to establish the RVWP (see Section 105 [6 U.S.C. 652]).

However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network. Through the Ransomware Vulnerability Warning Pilot (RVWP), which started on January 30, 2023, CISA is undertaking a new effort to warn critical infrastructure entities that their systems have exposed vulnerabilities that may be exploited by ransomware threat actors.

As part of RVWP, CISA leverages existing authorities and technology to proactively identify information systems that contain security vulnerabilities commonly associated with ransomware attacks. Once CISA identifies these affected systems, our regional cybersecurity personnel notify system owners of their security vulnerabilities, thus enabling timely mitigation before damaging intrusions occur.

CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including CISA's Cyber Hygiene Vulnerability Scanning service and the Administrative Subpoena Authority granted to CISA under Section 2209 of the Homeland Security Act of 2002.

FREQUENTLY ASKED QUESTIONS (FAQS)

Q: What is CIRCIA?

A: The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is federal legislation that puts in place requirements for critical infrastructure entities to report cyber incidents and ransom payments to CISA.

Q: Why is CISA sending me a notification?

A: CISA routinely identifies security risks facing U.S. organizations, including information from government or industry partners. CISA additionally leverages commercial tools to identify organizations that may be at heightened cybersecurity risk. As required by CIRCIA, CISA proactively identifies information systems that contain security vulnerabilities commonly associated with ransomware attacks. After discovery, CISA notifies owners of the vulnerable systems.

Q: Who will notify me if I have a vulnerability?

A: CISA Regional staff members, located throughout the country, make notifications and may provide assistance and resources to mitigate the vulnerability.

Q: What can I expect in the notification?

A: Notifications will contain key information regarding the vulnerable system, such as the manufacturer and model of the device, the IP address in use, how CISA detected the vulnerability, and guidance on how the vulnerability should be mitigated.

Q: How should I expect to receive a notification?

A: CISA regional staff members will make notifications by phone call or email.

Q: How do I verify it is CISA notifying me?

A: If you receive a notification, you can verify the identity of the CISA personnel through CISA Central: Central@cisa.gov or (888) 282-0870.

Q: If I received a notification, does that mean I was compromised?

A: Receiving a notification through CISA RVWP is not indicative of a compromise. However, it does indicate you are at risk and the information system requires immediate remediation.

Q: Am I required to comply with CISA's recommended actions?

A: No. Receiving a notification does not require you to comply with or institute any of CISA's recommendations.

Q: How did CISA determine I was vulnerable?

A: CISA leverages multiple open-source and internal tools to research and detect vulnerabilities within U.S. critical infrastructure.

Q: Can I receive other CISA services?

A: Absolutely! CISA offers multiple no-cost resources and tools. As a starting point, organizations should sign up for CISA's Cyber Hygiene Vulnerability Scanning, undertake a self-assessment to determine progress in implementing the Cybersecurity Performance Goals, and build a relationship with a regional CISA cybersecurity advisor to participate in additional applicable services or capabilities.