New Ransomware Vulnerability Warning Pilot

The Cybersecurity and Infrastructure Security Agency (CISA) has established the Ransomware Vulnerability Warning Pilot (RVWP) as authorized by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022. Through the RVWP, CISA will determine vulnerabilities commonly associated with known ransomware exploitation and warn critical infrastructure entities of those vulnerabilities, enabling mitigation before a ransomware incident occurs.

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents often perpetrated by cyber threat actors using known vulnerabilities. By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experience a ransomware event. However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network.

The RVWP will identify organizations with internet-accessible vulnerabilities commonly associated with known ransomware actors by using existing services, data sources, technologies, and authorities, including our free Cyber Hygiene Vulnerability Scanning service. CISA 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.

For more information on RVWP and other available resources for ransomware protection, detection, and response, all organizations are encouraged to visit StopRansomware.gov, a whole-of-government approach for ransomware resources and alerts.

Organizations interested with enrolling in CISA's Cyber Hygiene Vulnerability Scanning – contact vulnerability@cisa.dhs.gov.

For questions, please contact Cyber Security Advisor Jason Hemingway at JASON.HEMINGWAY@cisa.dhs.gov.