American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

December 1, 2023

URGENT: Hospital Action Needed to Protect Against 'Citrix Bleed' Vulnerability and Ransomware Threat

Hospitals and other critical infrastructure remain prime targets for cyberthreat that enables bypassing security measures to steal data and execute ransomware attacks

The Department of Health and Human Services' Health Sector Cybersecurity Coordination Center (HC3) is urging hospitals and other critical infrastructure to take immediate action to patch and harden network systems to protect against a significant ransomware threat, referred to as the "Citrix Bleed" vulnerability.

The Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Multi-State Information Sharing and Analysis Center and international partners on Nov. 21 alerted health care and other critical infrastructure organizations of the threat of the LockBit 3.0 ransomware gang exploiting this vulnerability, which allows cyberthreat actors to bypass password requirements and multifactor authentication measures.

"This urgent warning by HC3 signifies the seriousness to the Citrix Bleed vulnerability and the urgent need to deploy the existing Citrix patches and upgrades to secure our systems," said John Riggi, AHA's national advisor for cybersecurity and risk. "This situation also demonstrates the aggressiveness by which foreign ransomware gangs, primarily Russian-speaking groups, continue to target hospitals and health systems. Ransomware attacks disrupt and delay health care delivery, placing patient lives in danger. We must remain vigilant and harden our cyber defenses, as there is no doubt that cyber criminals will continue to target the field, especially during the holiday season. AHA also continues to implore the federal government to utilize all available resources and authorities across all agencies to conduct law enforcement actions and offensive cyber operations against these cyber terrorists."

WHAT YOU CAN DO

Citrix in early October released a patch for this vulnerability, but it has been reported that the vulnerability was being exploited as a zero-day since August 2023. Citrix also warned that these compromised sessions will still be active after a patch has been implemented. HC3 encourages all administrators to follow Citrix's guidance to upgrade their devices and remove any active or persistent sessions with the following commands:

- kill aaa session -all
- kill icaconnection -all

- kill rdp connection -all
- kill pcoipConnection -all
- clear lb persistentSessions

Additional guidance can be found in HC3 Nov. 30 Sector Alert 202311301200.

The FBI, CISA and MS-ISAC are providing tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Mitigation steps for hardening defenses against ransomware include:

- **Require** phishing-resistant multifactor authentication for all services to the extent possible, particularly for webmail, VPN and accounts that access critical systems.
- **Disable** command-line and scripting activities and permissions.
- **Implement** verbose and enhanced logging within processes, such as command-line auditing and process tracking.
- **Restrict** the use of PowerShell using Group Policy and only grant access to specific users on a case-by-case basis.
- **Update** Windows PowerShell or PowerShell Core to the latest version; uninstall all earlier PowerShell versions; and enable enhanced PowerShell logging.
- **Restrict** the use of RDP and other remote desktop services to known user accounts and groups.
- **Secure** remote access tools by:
    - Implementing application controls to manage and control execution of software, including allowlisting remote access programs.
    - Apply the recommendations in CISA's Joint Guide to Securing Remote Access Software.

Additional details on mitigation strategy can be found on CISA’s #StopRansomware page.

FURTHER QUESTIONS

If you have further questions, please contact Riggi at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.