Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

13 April 2021

PIN Number
20210413-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This product is marked TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

Cyber Attacks Targeting Network Servers Used by First Responders Can Slow and Disrupt Operational Response, Increase Safety Risks to Personnel

Summary

Cyber attacks, such as ransomware, can disrupt the availability of network servers and data used by emergency services personnel. This can delay access to real-time digital information, increasing safety risks to first responders and delaying response to calls for service. Public safety agencies across the US are increasingly adopting wireless connectivity and connected smart devices, both in vehicles and assigned to personnel, to provide first responders in the field the real-time information needed to conduct operations. These networks, connected devices, and the data transmitted are appealing targets for cyber actors. Cyber attacks against networks used by first responders can slow emergency response times, limit response to lower priority calls, and endanger first responders by sending them into situations with incomplete or incorrect information.

Threat Overview

Cyber actors targeting networks used by first responders can disrupt access to critical data, increase call response times, and may create cascading damage throughout the networks of state or local public safety agencies. These cyber attacks have the potential to impact connectivity for office-based personnel and the safety of those in the field who rely on connected technologies for information.

Since late 2018, the FBI has observed cyber actors conduct intrusions against networks used by first responders resulting in disrupted access to in-vehicle computers, reporting systems, e-mail systems, digital records of cases or arrests, fingerprinting databases, and criminal records. Cyber attacks have disrupted or encrypted 911 services and forced first responders to rely on manual record keeping for extended periods.

- In January 2021, a ransomware attack against a US city impacted the Computer Aided Dispatch (CAD) system, requiring the center to revert to manual dispatch. Multiple servers were impacted, including a server used for the 911 call handler recording device.
- In December 2020, an unidentified cyber actor conducted a ransomware attack on a US city's fire department, resulting in the encryption of a number of their systems. The department was able to restore their systems from viable backups, and did not pay the ransom.
- In late 2020, a US city emergency communications center was attacked with ransomware. Some servers were damaged and databases containing sensitive information were impacted. While the network was being remediated, alternative means for text notifications to first responders and the SWAT team had to be found. In addition, an unidentified cyber actor accessed the computer of a US city fire department through RDP and infected the network server with ransomware.
- In mid-2020, a 911 center experienced a telephony denial of service (TDoS) attack that impacted non-emergency lines. The TDoS attack prevented legitimate calls from being received, impacting the effectiveness of the center. During the same time period, an unidentified cyber actor conducted a separate ransomware attack on another US police department and encrypted servers. In-vehicle computers and electronic reporting systems could not be accessed.
- In late 2019, an unidentified cyber actor conducted a ransomware attack on a US sheriff's office and encrypted data on their servers. Office emails, arrest reports, fingerprinting, and criminal background checks were impacted.

Recommended Mitigations

- Ensure software and operating systems are updated regularly;
- Change default usernames and passwords of connected devices, modems, gateways and use strong passwords;
- Patch operating systems, software, firmware, and endpoints as vulnerabilities are discovered;
- Employ best practices for use of RDP, including auditing the network for systems using RDP, closing unused RDP ports, applying two-factor authentication and logging RDP login attempts;
- Maintain regular data back-ups that are separate from the network, and verify the integrity of the back-ups;
- Monitor vulnerabilities released by vendors of products used within a network boundary to stay up to date on current exposure. Vulnerability plugins are not always released in a timely fashion;
- Verify cybersecurity of devices before connecting them to networks or to vehicle area networks in the field;
- Protect administrator credentials and practice the principle of least privilege.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Administrative Note

This product is marked TLP:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey