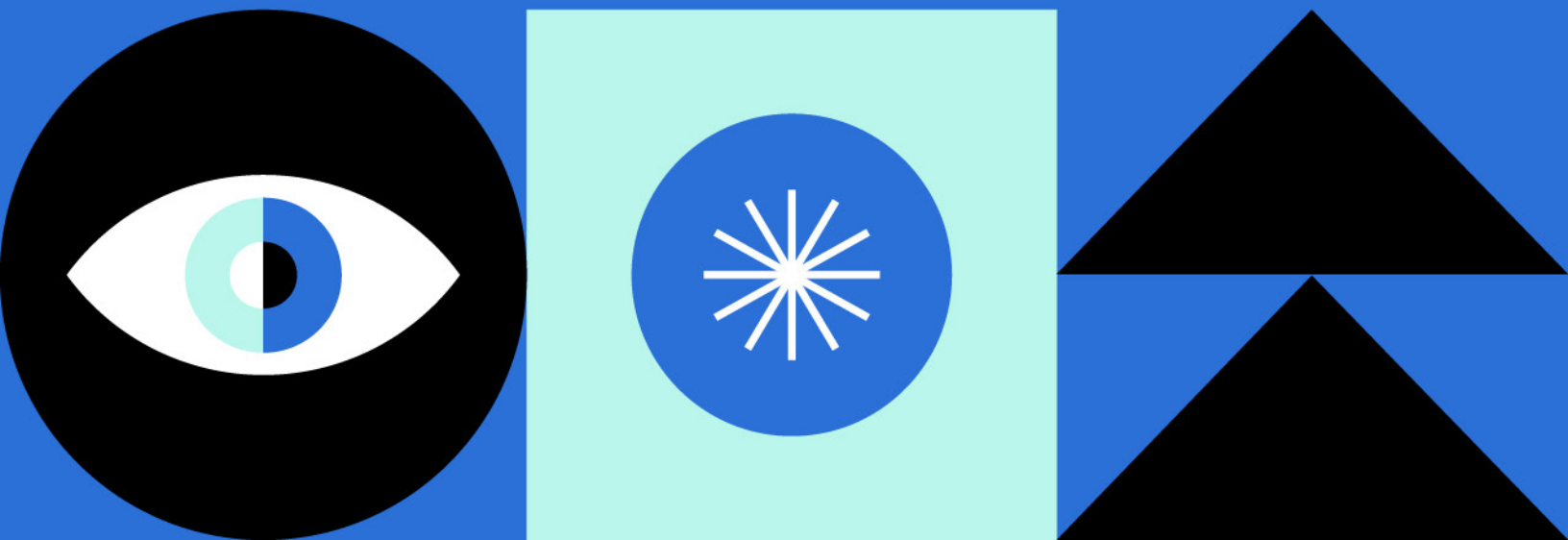
Coalition®

coalitioninc.com

Q1 2024

Quarterly Cyber Threat Bulletin



Top Cyber Threats

Thousands of vulnerabilities are discovered monthly, and many businesses need help with effective prioritizations and risk management. As part of our commitment to helping businesses stay informed and make good cybersecurity decisions, we present a roundup of the top cyber threats.

Table of Contents

THREAT #1

Ivanti Connect Secure

Affected systems or products

- Ivanti Connect Secure Virtual Private Network (VPN)
- Ivanti Policy Secure Gateways

Coalition Exploit Scoring System

- CVE-2023-46805: Authentication bypass vulnerability
- CVE-2024-21887: Command injection vulnerability

Description

On January 22, 2024, two significant vulnerabilities were identified in Ivanti devices, including an authentication bypass flaw (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887). These vulnerabilities could allow threat actors to gain unauthorized access and execute arbitrary commands on affected systems. On February 29, 2024, the Cybersecurity and Infrastructure Security Agency (CISA), in conjunction with other organizations, issued an updated threat advisory warning that threat actors were actively exploiting vulnerable Ivanti devices.

What can businesses do?

- Apply the Ivanti security patches as directed in the vendor advisory
- Conduct a thorough security audit of affected systems
- Limit Secure Sockets Layer (SSL) VPN connections to unprivileged accounts
- Review and update access control and network segmentation policies to minimize potential impact
- Monitor network traffic for unusual activity: new accounts, suspicious logins, privilege escalation attempts

Coalition response

Coalition is actively monitoring the situation and working closely to provide support and guidance. Coalition Incident Response (CIR), an affiliate of Coalition, Inc., proactively contacted policyholders known to be running Ivanti devices. Businesses running Ivanti devices that have noticed unusual network activity can contact Coalition for assistance.

Case study

A biotechnology company employing Ivanti devices detected a potentially malicious file. CIR[1] contacted the company as part of their outreach and partnered with the Head of IT to review logins and take mitigation steps. The company was also using managed detection and response (MDR) to monitor their network for suspicious activity. Because the biotech company took the alert seriously, swiftly responded to CIR outreach, and followed the necessary steps to mitigate the risk, it was able to successfully avoid a cyber incident.

1. Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.

THREAT #2

QR Code Phishing Campaigns

Affected systems or products

- Web Browsers
- Mobile Devices
- Software Applications

Risks

- Phishing
- Unauthorized Access
- Data Breach

Description

CIR has seen a recent increase in cyber insurance claims involving QR codes. Because QR codes are scanned using smartphones, they bypass security controls like endpoint detection and response (EDR). QR codes also bypass URL scanning performed by email providers.

What can businesses do?

- Educate employees about the risks of phishing as related to QR codes
- Avoid entering professional credentials on mobile devices unless explicitly directed to by a known member of the organization
- Consider implementing multi-factor authentication (MFA) to minimize the risk of unauthorized access
- Use secure web gateways and DNS filtering to block access to known phishing sites

Coalition response

Coalition Active Insurance policyholders[2] have access to up to two hours of pre-claims assistance with CIR.[3] This can be invaluable for businesses that receive suspicious emails with QR codes to assist in determining their risk.

Case study

A retail company experienced a security incident when employees scanned a QR code attached to an email from HR about their benefits, which directed them to a phishing site. Because the employee entered their credentials on the mobile phishing site the threat actor was able to elevate their access and lock all employees out of their Azure instance. CIR performed a full forensic investigation and the policyholder had to contact Microsoft to regain access to their Azure tenant. This incident underscores the importance of awareness as threat actors will often pivot tactics in an effort to avoid detection.

2. *Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc.("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through Coalition Insurance Company ("CIC") a licensed insurance underwriter (NAIC #29530). See licenses and disclaimers. Copyright © 2024. All rights reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.*
3. *Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.*

THREAT #3

ConnectWise ScreenConnect

Affected systems or products

- ConnectWise ScreenConnect 23.9.7 and prior

Coalition Exploit Scoring System

- CVE-2024-1708: Path-traversal vulnerability

Description

On February 19, 2024, ConnectWise disclosed critical vulnerabilities in its ScreenConnect software, potentially enabling remote code execution or compromising confidential data. The vulnerabilities include an authentication bypass (CWE-288) and improper limitation of a pathname (CWE-22). Additionally, the LockBit ransomware gang has been observed exploiting both vulnerabilities.

What can businesses do?

- Update all versions of ConnectWise ScreenConnect to version 23.9.8, which contains patches for the identified vulnerabilities
- Implement network segmentation and restrict access to the ScreenConnect interface to minimize exposure
- Conduct regular security audits and vulnerability assessments to identify and mitigate potential weaknesses in the network infrastructure

Coalition response

Coalition is actively monitoring the situation and working closely with affected parties to provide support and guidance.

Case study

As of March 6, 2024, CIR has handled eight ransomware cases in which attackers exploited the ScreenConnect vulnerabilities. After analyzing the indicators of compromise (IOCs), CIR determined five were associated with a version of LockBit 3.0, the ransomware binary associated with LockBit, and three were pre-encryption. LockBit was previously the subject of an FBI takedown, but it is not possible to confirm if these cases indicate an affiliate threat actor or a rebrand by the group. During forensic investigations, CIR observed that all pre-encryption cases had EDR deployed. Detection and response technology can help enhance organizations' security postures, and CIR routinely uses EDR solutions during the restoration phase.

THREAT #4

FortiOS SSL VPN

Affected systems or products

- FortiOS SSL VPN Gateways

Coalition Exploit Scoring System

- CVE-2024-21762: Out-of-bounds write

Description

On February 8, 2024, a critical vulnerability was identified in FortiOS SSL VPN that could allow an unauthenticated attacker to execute arbitrary code remotely on affected devices. This flaw could potentially grant threat actors unauthorized access to sensitive information. On February 9, 2024, the CISA added the FortiOS SSL VPN vulnerability to its Known Exploited Vulnerabilities (KEV) catalog and announced attackers were actively exploiting it in the wild.

What can businesses do?

- Apply the latest Fortinet patches for FortiOS SSL VPN appliances
- Review and strengthen firewall rules and VPN configurations to limit exposure to potential exploits

Coalition response

Coalition is actively monitoring the situation and working closely with affected parties to provide support and guidance. Coalition external scans cannot detect which firmware version a business is running. Any policyholder with questions or concerns regarding their Fortinet device or the FortiOS SSL VPN vulnerability can contact our Security Support Center.

THREAT #5

Cisco ASA and FTD Devices

Affected systems or products

- Cisco Adaptive Security Appliance (ASA) Devices
- Cisco Firepower Threat Defense (FTD) Software

Coalition Exploit Scoring System

- CVE-2020-3259: Memory contentleak vulnerability targeted by Akira Ransomware
- CVE-2020-3452: Directory traversal vulnerability in ASA and FTD

Description

In late 2023, Truesec security researchers discovered ransomware gang Akira was actively exploiting a Cisco ASA vulnerability from 2020. This vulnerability allows an unauthenticated, remote threat actor to retrieve sensitive memory content of the system, including passwords. Cisco has released an updated vendor advisory for this vulnerability.

These vulnerabilities not only compromise the security of Cisco ASA and FTD devices but also expose organizations to significant risks of data breaches and ransomware attacks.

What can businesses do?

- Follow Cisco's recommendations and update to the latest supported firmware
- Consider implementing multi-factor authentication (MFA) on all VPN access points to mitigate the risk of unauthorized access

Coalition response

Coalition is actively monitoring the situation and working closely with affected parties to provide support and guidance. Any policyholder with questions or concerns regarding their Cisco ASA device or the Cisco ASA vulnerability can contact our Security Support Center.

Stay Ahead of Cyber Threats

As a leading provider of cyber insurance and risk management services, Coalition has a unique vantage point on the risks that matter most and how businesses can remediate them. We often publish security alerts and other content on emerging cyber threats on our blog: coalitioninc.com/blog

Coalition Security Services offers tailored solutions for small and medium businesses that can help them scale their response to fast-moving digital threats. Coalition Managed Detection and Response (MDR)[4] offers round-the-clock threat detection and response to help businesses react quickly to cyber attacks as well as new and emerging vulnerabilities. Contact mdr@coalitioninc.com for more information

4. Coalition Security Services MDR services are provided by Coalition Incident Response, Inc., an affiliate of Coalition.