Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

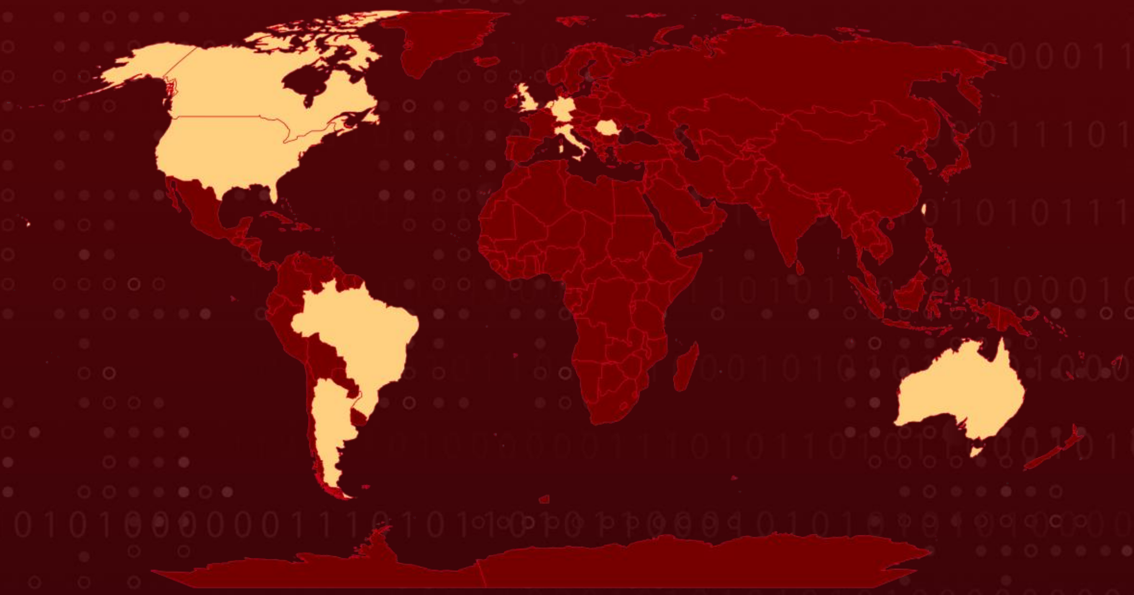
Akira Ransomware Exploits Cisco Flaw for Maximum Impact

Date of Publication	Admiralty Code	TA Number
February 19, 2024	A2	TA2024064

Summary

Attack Commenced: January 2024
Malware: Akira Ransomware
Attack Region: United States, Romania, Argentina, Canada, Taiwan, Netherlands, Italy, Brazil, United Kingdom, Australia, Germany
Targeted Industries: Automotive, Manufacturing, Education, Technology, Internet Software and services, Professional Services, Design, Legal, Hospitality, Financial, Travel, Telecommunications, Real Estate, Retail, Charitable Organizations, Pharmaceutical, Environmental Contracting, Construction and engineering, Transportation, Agriculture, Energy, Packaging
Attack: The Akira ransomware has been identified for utilizing the Cisco AnyConnect SSL VPN as its initial access vector, specifically exploiting the CVE-2020-3259 vulnerability. Despite Cisco addressing this vulnerability with patches released in May 2020, the threat remains prevalent.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-3259	Cisco ASA and FTD Information Disclosure Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	✗	✓	✓

Attack Details

#1 The Akira ransomware was deployed, utilizing the Cisco AnyConnect SSL VPN as the initial access vector. For this vulnerability to be exploited, the device with the susceptible software must have the AnyConnect SSL VPN enabled on the interface exposed to potential attackers.

#2 The identified vulnerability is CVE-2020-3259, an information disclosure issue that could potentially allow an attacker to retrieve the contents of the device's memory. Additionally, it is a common modus operandi for attackers to exploit the same device multiple times, thereby gaining access to various segments of the memory content. Cisco addressed this vulnerability through patches released in May 2020.

#3 Over the past year, actors associated with the Akira ransomware have weaponized multiple vulnerable Cisco AnyConnect SSL VPN appliances. Exploiting this vulnerability allows attackers to extract sensitive data from the memory of affected devices, including usernames and passwords.

#4 Notably, Akira and Lockbit ransomware groups are actively attempting to breach Cisco ASA SSL VPN devices by exploiting several older vulnerabilities, some of which have had patches available since 2020 and 2023. System administrators are strongly advised to upgrade to the latest ASA release on all devices featuring the AnyConnect SSL VPN, especially those with an internet-exposed interface.

Recommendations

Immediate Patching: System administrators are strongly advised to apply the patches released by Cisco to address the CVE-2020-3259 vulnerability in the AnyConnect SSL VPN. Patching is crucial to prevent potential exploits by Akira and other ransomware groups.

Enable Multi-Factor Authentication (MFA): Implement MFA across all accounts and services, with a particular emphasis on Client VPN connections. This adds a layer of security, making it more challenging for unauthorized access.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Implement Network Security Measures: Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0007** Discovery
TA0011 Command and Control	**TA0040** Impact	**T1588.006** Vulnerabilities	**T1596** Search Open Technical Databases
T1190 Exploit Public-Facing Application	**T1486** Data Encrypted for Impact	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1562 Impair Defenses	**T1059** Command and Scripting Interpreter	**T1041** Exfiltration Over C2 Channel	**T1082** System Information Discovery
T1057 Process Discovery	**T1055** Process Injection	**T1490** Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f, f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92, ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af, aca0f5e76dacc4b9145c17a25a639aeb2e4cf76b7859bcb27224c42e404013a2, 08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba, ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab, 030db5fb2a639b0c1a63bbd209bd1f043dbc4dbb306102f1726cdd4a6500fb83, b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2, 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3, 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db, 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4, 5009343ce7e6e22a777b22440480fe2eb26098d4a2ecc62e6df4498819e26b5c

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

Recent Breaches

https://www.bramauto.com
https://www.asam.com
https://www.nekoosaschools.org
https://www.sanokrubber.com
https://www.distecna.com
https://www.terago.ca
https://www.aver.com
https://www.celeste.com
https://www.vcsobservation.com
https://www.gruskingroup.com
https://www.borahgoldstein.com
https://www.riverscasino.com
https://www.sefin.com
https://www.safeplating.com
https://www.castilleja.org
https://www.getawaytoday.com
https://www.valleytelecomgroup.com
https://www.brazilianbusinesspark.com
https://www.ani-networks.com
https://www.lush.com
https://www.torontozoo.com
https://www.dirigsheetmetal.com
https://www.wilhoitproperties.com
https://www.cryopak.com
https://www.milestoneenvironmentalcontracting.com
https://www.hmhonline.org
https://www.hydratek.com
https://www.denhamthejeanmaker.com
https://www.tgstransportation.com
https://www.bestwaysales.com
https://www.premiumguard.com
https://www.beckerlogistics.com
https://www.nissan.com.au
https://www.vincentznetwork.com
https://www.blackburn.ac.uk
https://www.viridi.energy
https://www.itopallpackgruppen.com
https://www.hellerindustries.com
https://www.vanburenschools.net

References

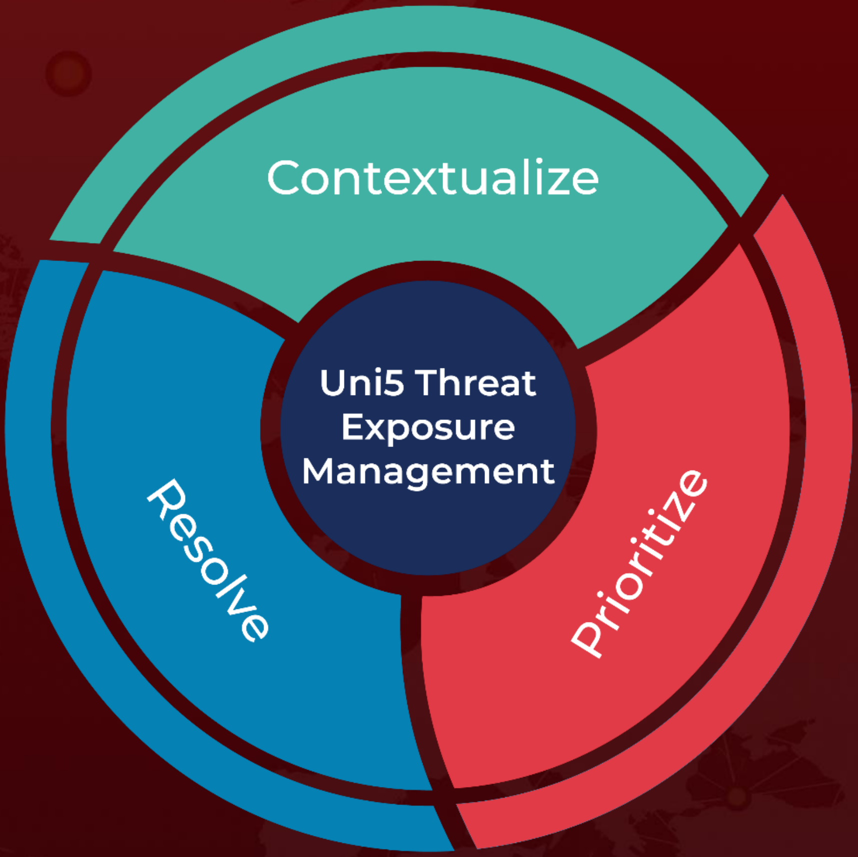
https://www.truesec.com/hub/blog/akira-ransomware-and-exploitation-of-cisco-anyconnect-vulnerability-cve-2020-3259

https://www.hivepro.com/threat-advisory/new-wave-of-akira-ransomware-expands-arsenal-with-cisco-vpn-flaws/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 19, 2024 • 5:30 PM

More at www.hivepro.com