Hive Pro

Threat Level

Red

CISA: AA23-108

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

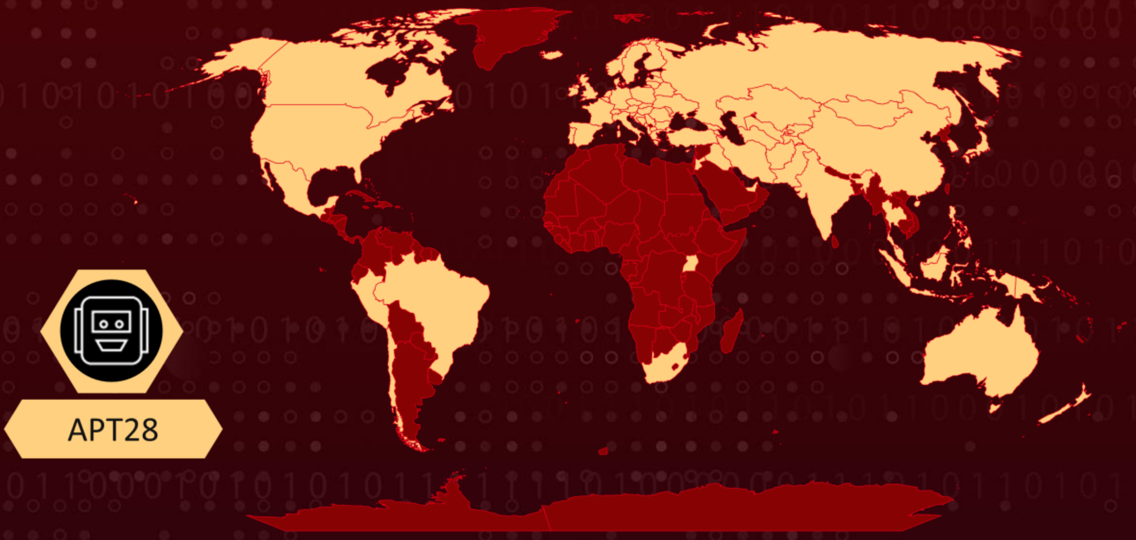
APT28's SNMP Attack on Cisco Routers

Date of Publication	Admiralty Code	TA Number
April 24, 2023	A1	TA2023196

Summary

Attack began: 2021
Threat Actor: APT28(Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium , Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12 , ITG05, TAG-0700, UAC-0028, Grey-Cloud)
Malware: Jaguar Tooth
Affected Product: Cisco routers
Attack Countries: Afghanistan, Albania, Andorra, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Brunei, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Holy See, Hong Kong, Hungary, Iceland, India, Indonesia, Iran, Iraq, Ireland, Italy, Japan, Jordan, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Moldova, Monaco, Mongolia, Montenegro, Netherlands, New Zealand, North Macedonia, Norway, Pakistan, Papua New Guinea, Peru, Philippines, Poland, Portugal, Republic of Korea, Romania, Russia , San Marino, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taipei, Tajikistan, Thailand, Turkey, Türkiye, Turkmenistan, UAE, Uganda, UK, Ukraine, USA, Uzbekistan.
Attack Industry: Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.
Attack: APT28 used SNMP access to exploit Cisco routers and gain network access, utilizing weak SNMP community strings and exploiting a vulnerability to deploy Jaguar Tooth and obtain further device information.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-6742	Cisco SNMP Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓

Attack Details

#1 In 2021, APT28 used SNMP access to gain entry into Cisco routers around the world, allowing them to access router information and exploit devices to penetrate a network. To do this, APT28 sent additional SNMP commands to enumerate router interfaces. The routers that were compromised were configured to accept SNMP v2 requests, which don't support encryption. Weak SNMP community strings, such as the default "public," made it easy for APT28 to gain access to router information.

#2 APT28 also exploited CVE-2017-6742, a vulnerability that Cisco announced on June 29, 2017. For some of the targeted devices, APT28 used an SNMP exploit to deploy malware, which gave them further device information and enabled unauthenticated access via a backdoor. APT28 was able to obtain device information by executing CLI commands via the malware, including the discovery of other devices on the network by querying the ARP table to obtain MAC addresses.

Recommendations

Follow Cisco's advice for patching devices and ensure that software is kept up-to-date. If SNMP is not necessary for remote device management, it should be disabled to prevent unauthorized access. If SNMP is required, configure allow and deny lists for SNMP messages and use SNMP v3 or other encrypted protocols wherever possible.

To detect any potential compromise, it is recommended to utilize the detection rules provided by CISA.

Use logging tools like TACACS+ and Syslog to record commands executed on network devices and be sure to monitor logs for suspicious activity. If a router has been compromised, follow Cisco's advice for verifying the IOS image and revoke all keys associated with the device. In such cases, replace both the ROMMON and IOS image with a version sourced directly from Cisco's website.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0005 Defense Evasion	TA0009 Collection
TA0010 Exfiltration	TA0007 Discovery	T1190 Exploit Public-Facing Application	T1078 Valid Accounts
T1078.001 Default Accounts	T1590 Gather Victim Network Information	T1556 Modify Authentication Process	T1601 Modify System Image
T1601.001 Patch System Image	T1048 Exfiltration Over Alternative Protocol	T1048.003 Exfiltration Over Unencrypted Non-C2 Protocol	T1020 Automated Exfiltration
T1119 Automated Collection	T1602 Data from Configuration Repository	T1602.002 Network Device Configuration Dump	T1018 Remote System Discovery
T1083 File and Directory Discovery	T1016 System Network Configuration Discovery	T1082 System Information Discovery	

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

References

https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jaguar-tooth/NCSC-MAR-Jaguar-Tooth.pdf

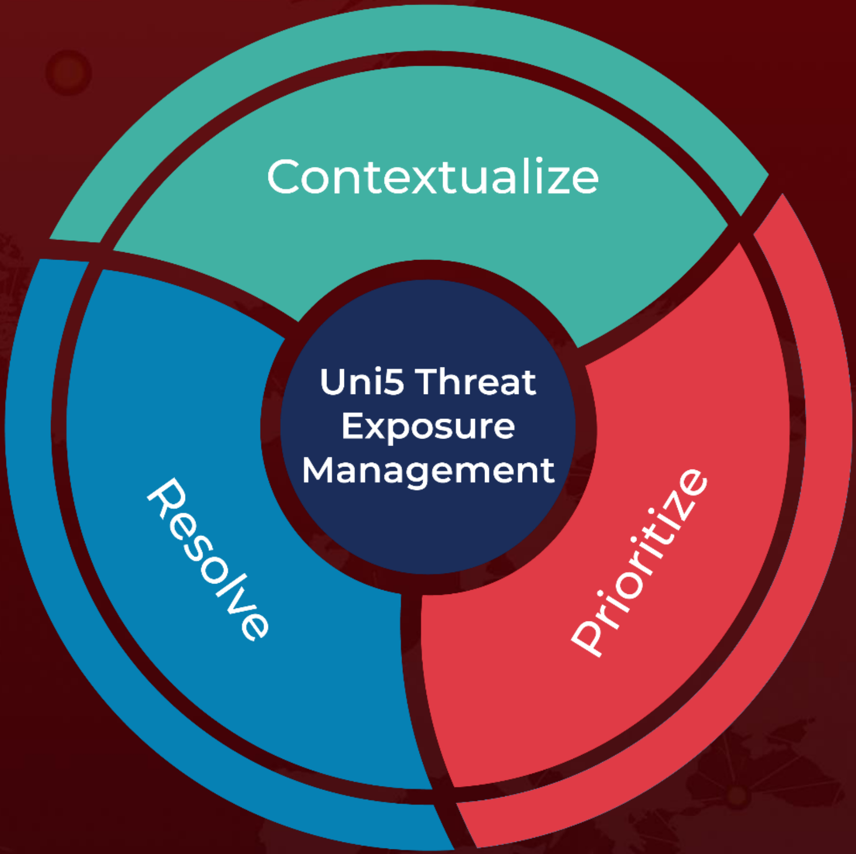
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

https://blogs.cisco.com/security/threat-actors-exploiting-snmp-vulnerabilities-in-cisco-routers

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

April 24, 2023 • 5:45 AM

More at www.hivepro.com