National Cyber Security Centre
a part of GCHQ

Advisory.

APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers

Version 1

18 April 2023

APT28 exploits known vulnerability to carry out reconnaissance of routers and deploy malware

APT28 accesses poorly maintained Cisco routers and deploys malware on unpatched devices using CVE-2017-6742.

Overview and context

The UK National Cyber Security Centre (NCSC), the US National Security Agency (NSA), US Cybersecurity and Infrastructure Security Agency (CISA) and US Federal Bureau of Investigation (FBI) are releasing this joint advisory to provide details of tactics, techniques and procedures (TTPs) associated with APT28's exploitation of Cisco routers in 2021.

We assess that APT28 is almost certainly the Russian General Staff Main Intelligence Directorate (GRU) 85th special Service Centre (GTsSS) Military Intelligence Unit 26165. APT28 (also known as Fancy Bear, STRONTIUM, Pawn Storm, the Sednit Gang and Sofacy) is a highly skilled threat actor.

Previous activity

The NCSC has previously attributed the following activity to APT28:

- cyber attacks against the German parliament in 2015, including data theft and disrupting email accounts of German Members of Parliament (MPs) and the Vice Chancellor
- attempted attack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in April 2018, to disrupt independent analysis of chemicals weaponised by the GRU in the UK

For more information on APT28 activity, see the advisory 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure' and 'Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments'

As of 2021, APT28 has been observed using commercially available code repositories, and post-exploit frameworks such as Empire. This included the use of Powershell Empire, in addition to Python versions of Empire.

Reconnaissance

Use of SNMP protocol to access routers

In 2021, APT28 used infrastructure to masquerade Simple Network Management protocol (SNMP) access into Cisco routers worldwide. This included a small number based in Europe, US government institutions and approximately 250 Ukrainian victims.

SNMP is designed to allow network administrators to monitor and configure network devices remotely, but it can also be misused to obtain sensitive network information and, if vulnerable, exploit devices to penetrate a network.

A number of software tools can scan the entire network using SNMP, meaning that poor configuration such as using default or easy-to-guess community strings, can make a network susceptible to attacks.

Weak SNMP community strings, including the default 'public', allowed APT28 to gain access to router information. APT28 sent additional SNMP commands to enumerate router interfaces. [T1078.001]

The compromised routers were configured to accept SNMP v2 requests. SNMP v2 doesn't support encryption and so all data, including community strings, is sent unencrypted.

Exploitation of CVE-2017-6742

APT28 exploited the vulnerability CVE-2017-6742 (Cisco Bug ID: CSCve54313) [T1190]. This vulnerability was first announced by Cisco on 29 June 2017, and patched software was made available.

Cisco's published advisory provided workarounds, such as limiting access to SNMP from trusted hosts only, or by disabling a number of SNMP Management Information bases (MIBs).

Malware deployment

For some of the targeted devices, APT28 actors used an SNMP exploit to deploy malware, as detailed in the NCSC's **Jaguar Tooth malware analysis report.** This malware obtained further device information, which is exfiltrated over trivial file transfer protocol (TFTP), and enabled unauthenticated access via a backdoor.

The actor obtained this device information by executing a number of Command Line Interface (CLI) commands via the malware. It includes discovery of other devices on the network by querying the Address Resolution Protocol (ARP) table to obtain MAC addresses [T1590]

Indicators of compromise (IoCs)

Please refer to the accompanying malware analysis report for indicators of compromise which may help to detect this activity.

MITRE ATT&CK®

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

For detailed TTPs, see the malware analysis report.

Tactic	ID	Technique	Procedure
Initial Access	T1190	Exploit Public-facing Application.	APT28 exploited default/well-known community strings in SNMP as outlined in CVE-2017-6742 (Cisco Bug ID: CSCve54313)
Initial Access	T1078.001	Valid Accounts. Default Accounts.	Actors accessed victim routers by using default community strings such as 'public'
Reconnaissance	T1590	Gather victim network information	Access was gained to perform reconnaissance on victim devices. Further detail of how this was achieved in available in the MITRE ATT&CK section

```
                                                    of the Jaguar Tooth
                                                    MAR
```

Conclusion

APT28 has been known to access vulnerable routers by using default and weak SNMP community strings, and by exploiting CVE-2017-6742 (Cisco Bug ID: CSCve54313) as published by Cisco.

TTPs in this advisory may still be used against vulnerable Cisco devices. Organisations are advised to follow the mitigation advice in this advisory to defend against this activity.

Reporting

UK organisations should report any suspected compromises to the NCSC.

US organisations should contact CISA's 24/7 Operations Centre at Report@cisa.gov or (888) 282-0870

Mitigation

- Patch devices as advised by Cisco. The NCSC also has general guidance on managing updates and keeping software up to date.

- Do not use SNMP if you are not required to configure or manage devices remotely to prevent unauthorised users from accessing your router.
    - If you are required to manage routers remotely, establish allow and deny lists for SNMP messages to prevent unauthorised users from accessing your router.

- Do not allow unencrypted (ie, plaintext) management protocols, such as SNMP v2 and Telnet. Where encrypted protocols aren't possible, you should carry out any management activities from outside the organisation through an encrypted virtual private network (VPN), where both ends are mutually authenticated.

- Enforce a strong password policy. Don't reuse the same password for multiple devices. Each device should have a unique password. Where possible, avoid legacy password-based authentication and implement two-factor authentication based on public-private key.

- Disable legacy unencrypted protocols such as Telnet and SNMP v1 or v2c. Where possible, use modern encrypted protocols such as SSH and SNMP v3. Harden the encryption protocols based on current best security practice. The NCSC strongly advises owners and operators to retire and replace legacy devices that can't be configured to use SNMP v3.

- Use logging tools to record commands executed on your network devices, such as TACACS+ and Syslog. Use these logs to immediately highlight suspicious events and keep a record of events to support an investigation if the device's integrity is ever in question. See NCSC guidance on monitoring and logging.

- If you suspect your router has been compromised:
    - Follow Cisco's advice for verifying the Cisco IOS image.
    - Revoke all keys associated with that router. When replacing the router configuration be sure to create new keys rather than pasting from the old configuration.

- Replace both the ROMMON and Cisco IOS image with an image that has been sourced directly from the Cisco website, in case third party and internal repositories have been compromised.

- NSA's Network Infrastructure guide provides some best practices for SNMP.
- See also the Cisco IOS hardening guide and Cisco's Jaguar Tooth blog.