Cyber Threats

Monthly Cyber Intelligence Summary

November 2024

Mishcon de Reya

It's business. But it's personal.

November 2024 - Cyber Threat Update

Incident	Threat	Key points
Russian spear-phishing email campaign across government and IT in UK, Europe, Australia, and Japan.	Emails contained RDP files that allowed the attackers to access and potentially steal sensitive data from the victims' networks, and possibly install malware or maintain unauthorised access.	Simple yet effective attack can be used by multiple threat actors. Defenders are advised to implement multiple security measures, including firewalls, MFA, and antivirus protections, to mitigate such threats.
Cisco industrial wireless software vulnerability allows attackers root command execution.	Cisco patched a critical vulnerability affecting specific industrial models which allowed command execution with root access via crafted HTTP requests. No active exploitation has been reported.	It is advised to update Cisco devices to fix this vulnerability and prevent root access attacks. Admins need to install patches, check settings, and monitor for breaches. Ongoing security involves regular checks, layered defences, and staff training.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

1. The document has three main purposes to assist cybersecurity leaders:
2. To be 'threat-led' and help prioritise defences against particular types of attackers
3. To justify business decisions on cybersecurity changes, technology or services

To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Simple yet effective RDP spear-phishing campaign

What happened?

On 31 October, the US Cybersecurity and Infrastructure Security Agency (CISA) warned about a "foreign threat actor" targeting over 100 government and IT companies with an email campaign utilising malicious Remote Desktop Protocol (RDP) files to gain access to files stored on the target's network.[1] The activity targeted dozens of countries but particularly the UK, those in Europe, Australia, and Japan. Other sectors targeted included higher education, defence and non-governmental organisations (NGOs).

The campaign involved sending highly targeted spear-phishing emails with signed RDP configuration files that connected the victims' devices to an actor-controlled server and bidirectionally mapped the targeted user's local device's resources to the server. The emails impersonated Microsoft employees and referenced other cloud providers to add credibility.

Resources sent to the server may have included, but were not necessarily limited to, all logical hard disks, clipboard contents, printers, connected peripheral devices, audio, and authentication features and facilities of the Windows operating system, including smart cards.

This access could enable the threat actor to install malware on the target's local drive(s) and mapped network share(s), particularly in AutoStart folders, or install additional tools such as remote access trojans (RATs) to maintain access when the RDP session is closed. The process of establishing an RDP connection to the actor-controlled system may also expose the credentials of the user signed in to the target system.

Microsoft attributed the campaign to threat actor "Midnight Blizzard" (also known as APT29). The group are associated with the SVR (Foreign Intelligence Service of the Russian Federation), and known for intelligence collection since early 2018, using various methods like spear-phishing, stolen credentials, and supply chain attacks.

Similar attacks were reported by Microsoft, the Government Computer Emergency Response Team of Ukraine[2] (CERT-UA) and Amazon[3].

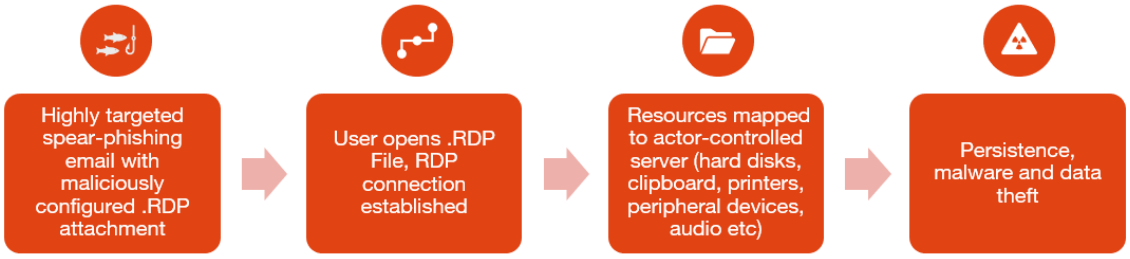

Figure 1 - Stages of the attack

[1] Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments, https://www.cisa.gov/news-events/alerts/2024/10/31/foreign-threat-actor-conducting-large-scale-spear-phishing-campaign-rdp-attachments
[2] RDP configuration files as a means of obtaining remote access to a computer, https://cert.gov.ua/article/6281076
[3] Amazon identified internet domains abused by APT29, https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/

So what?

While the targeting of this campaign is indicative of an intelligence-gathering operation for the purposes of espionage, the technique is surprisingly simple yet effective so can be applied by multiple threat actors including those involved in financially motivated crimes. Hence the use of this technique should be considered by all network defenders.

Mitigations include "defence in depth" approaches which allow for multiple layers of security controls to detect and mitigate the impact. A full list of controls and threat hunting artefacts have been published by Microsoft[4], but pertinently:

Strengthen operating environments:

- Use Windows Firewall to restrict outbound RDP connections.
- Implement multifactor authentication (MFA), especially phishing-resistant methods like FIDO Tokens or Microsoft Authenticator.
- Use Conditional Access to require strong authentication for critical apps.
- Encourage the use of browsers with Microsoft Defender SmartScreen to block malicious sites.

Strengthen endpoint security:

- Enable tamper protection in Microsoft Defender for Endpoint.
- Activate network and web protection features.
- Use endpoint detection and response (EDR) in block mode to stop threats.
- Set up automated investigation and remediation to resolve breaches quickly.
- Apply attack surface reduction rules to prevent common attack techniques.

Enable Safe Links and Safe Attachments:

- Use Zero-hour auto purge (ZAP) to neutralize threats in delivered emails.

Strengthen antivirus configuration:

- Turn on cloud-delivered protection and real-time protection in Microsoft Defender Antivirus.
- Ensure scanning of downloaded files and attachments is enabled.

[4] Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files, https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

Vulnerability in Cisco industrial wireless software enables attackers to execute commands with root privileges

What happened?

On 6th November 2024, Cisco addressed a critical vulnerability designated as CVE-2024-20418, categorised at the highest level of severity. This has affected certain models of its Ultra-Reliable Wireless Backhaul (URWB) access points used in industrial wireless automation.

URWB are devices that enable stable, high-speed wireless data transfer over long distances, designed for use where cable connections are not viable. The flaw was in the web-based management interface of Cisco's Unified Industrial Wireless Software and could be exploited by unauthenticated attackers without the need for user interaction.[5]

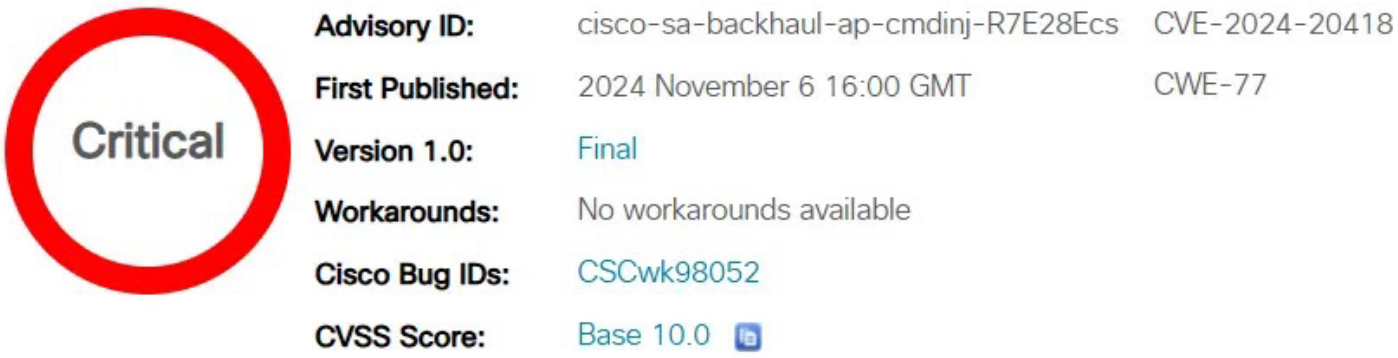

Figure 2 : CVE Profile (Source: Cisco)

The vulnerability arises from insufficient validation of input to the web-based management interface. Attackers could exploit this by sending specially crafted HTTP requests, leading to the execution of commands with root privileges on the operating system of the affected device.[6] Root privileges means that attackers can potentially gain the highest level of access to a system, leading to full control.

The specific models impacted by this vulnerability include the Catalyst IW9165D Heavy Duty Access Points, Catalyst IW9165E Rugged Access Points and Wireless Clients, and Catalyst IW9167E Heavy Duty Access Points. However, the vulnerability only affects devices running susceptible software with the URWB operating mode enabled.[7]

---

[5] Critical bug in Cisco UWRB access points allows attackers to run commands as root
https://securityaffairs.com/170646/security/cisco-uwrb-cririca l-flaw.html?web_view=true
[6] Cisco bug lets hackers run commands as root on UWRB access points
https://www.bleepingcomputer.com/news/security/cisco-bug-lets-hackers-run-commands-as-root-on-uwrb-access-points/
[7] Cisco Industrial Wireless Software Flaw Let Attackers Run Command As Root User
https://cybersecuritynews.com/cisco-flaw-attackers-command-root-user/

So far, Cisco's Product Security Incident Response Team (PSIRT) has not found any evidence of public exploit code availability or active exploitation of this critical security flaw, however, it is likely that this will change in future.

So what?

This vulnerability is a critical reminder for organisations to maintain vigilance and promptly apply security updates to their network infrastructure. The ability for attackers to gain root access poses a severe risk to network integrity and operational continuity, especially in industrial environments where reliability is paramount.

Administrators responsible for the maintenance of Cisco devices should:

- Apply the provided updates from Cisco immediately.
- Verify whether the URWB operating mode is enabled by using the "show mpls-config" CLI command and take appropriate measures if necessary.
- Continuously monitor for any signs of compromise or unusual network activity.

In addition to these immediate actions, organisations should:

- Ensure regular security assessments and penetration testing are conducted.
- Adopt a defence-in-depth strategy to protect against various cyber threats.
- Train staff to recognise and respond to security incidents effectively.

The proactive management of vulnerabilities is essential in safeguarding against potential exploitation and minimising the risk of operational disruption. Organisations should stay informed about the latest security advisories and implement recommended security measures to strengthen their cyber defences.

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com/cyber-risk-and-complex-investigations

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.