MDR CYBER
Part of the Mishcon de Reya Group

April 2024

Cyber Threats

Monthly Cyber Intelligence Summary

mishcon.com/cyber

April 2024 – Cyber Threat Update

Summary

Incident	Threat	Key points
Backdoor discovered in Linux XZ Utils software allowing remote code execution.	The backdoor was introduced by a long-time trusted contributor, raising concerns about a potential state-sponsored sophisticated attack.	Linux users are advised to update or downgrade XZ Utils to a secure version and refer to US CISA and Red Hat for detailed guidance.
Password-spraying reconnaissance attacks target Cisco Remote Access VPN services.	The attacks, potentially from the Brutus botnet and linked to suspected Russian state-sponsored groups, involve trying the same password across multiple accounts for unauthorised access.	Attacks can be detected through monitoring for high numbers of failed authentication attempts. Best practice includes sink holing and blocking IPs or using certificate-based authentication.

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.

The document has three main purposes to assist cybersecurity leaders:

1. To be 'threat-led' and help prioritise defences against particular types of attackers
2. To justify business decisions on cybersecurity changes, technology or services
3. To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Update Linux systems to protect against XZ Utils supply chain attack

What?

On 29 March, a Microsoft software developer inadvertently discovered a SSH (Secure Shell Protocol) backdoor in the XZ Utils data compression utility used by multiple Linux-based applications.[1] Linux is an open-source operating system that underpins many commercial networking devices and is widely used. Vulnerable versions discovered include 5.6.0 and 5.6.1.[2]

The backdoor, assigned as CVE-2024-3094, allows remote code execution by unauthenticated attackers meaning that devices with the vulnerable software, which comes as standard in many Linux distributions, are at risk of access and exploitation. Proof-of-concept (PoC) code was reportedly made publicly available, meaning that exploitation was also more likely due to PoC ready availability.

While the full details of the origins of the exploit are subject to speculation, the malicious code was introduced by a user calling themselves Jia Tian, who had contributed to the XZ project for several years and who built trust with other developers who had contributed to the project. The user had reportedly achieved sufficient trust to be able to contribute code without approval from others. There are indications that the community of developers were socially engineered to allow the insertion of the code. The stealth, longevity and sophistication of the software supply chain compromise has led some to speculate that the attackers were state sponsored, although this is not clear nor confirmed.

So what?

Remediation steps for various Linux systems have been made available per Linux version.[3][4] Generally, the advice is to check if you are running a vulnerable version and upgrade to the latest. Security vendor JFrog also released a tool to check if a machine is vulnerable and affected, although please note that we have not independently tested this.[5]

Where fixes may not be available yet, users may be advised to downgrade XZ Utils to an uncompromised version. We advise that users check definitive sources of advice including the US CISA guidance[6] and the Red Hat advice to ensure that they are protected.[7]

If upgrading is not possible, the backdoor can be disabled by adding the string "yolAbejyiejuvnup=Evjtgvsh5okmkAvj" to /etc/environment and restarting, which utilises the backdoor's kill switch.

[1] The Other Players Who Helped (Almost) Make The World's Biggest Backdoor Hack https://theintercept.com/2024/04/03/linux-hack-xz-utils-backdoor/

[2] Critical Vulnerability in XZ Utils for Linux https://digital.nhs.uk/cyber-alerts/2024/cc-4473

[3] Critical Vulnerability in XZ Utils for Linux https://digital.nhs.uk/cyber-alerts/2024/cc-4473

[4] CVE-2024-3094 XZ Backdoor: All you need to know, https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/

[5] CVE-2024-3094 (XZ Backdoor) Detector, https://github.com/jfrog/cve-2024-3094-tools/tree/main/cve-2024-3094-detector

[6] Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094, https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094

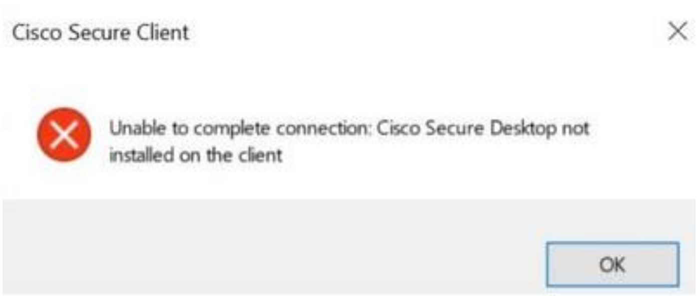
[7] CVE-2024-3094, https://access.redhat.com/security/cve/CVE-2024-3094

Cisco provides best practice guidance on countering password-spraying attacks against VPNs

What?

On 26 March Cisco released an advisory warning of multiple reports of password-spraying attacks aimed at Remote Access VPN (RAVPN) services configured on Cisco Secure Firewall ASA and Secure Firewall Threat Defence (FTD) devices. The activity reportedly targeted other VPN services and was part of what they assessed to be reconnaissance activity. Password spraying is when attackers try the same password, typically in an automated way, against multiple accounts to attempt to log in.

The activity was characterised by users who were unable to connect to Cisco Secure Client (AnyConnect) and met with an error prompt stating "*Unable to complete connection. Cisco Secure Desktop not installed on the client*".



Unable to complete connection: Cisco Secure Desktop not installed on the client

Figure 1 - Error prompt

A security researcher assessed that the activity likely emanated from the Brutus botnet, which they had observed since mid-March and used around 20 thousand IP addresses worldwide, from various infrastructure including cloud services and residential IPs.[8] The operators of the botnet are unknown, but it has been associated with two suspected Russian state-sponsored groups.

So what?

To counter the impact of the attempts, Cisco provided a series of recommendations, some of which also provide general best practice. This includes enabling Cisco ASA and FTD software logging so that attacks can be detected, securing VPN profiles by configuring a dummy Lightweight Directory Access Protocol (LDAP) server to sinkhole the attempts and blocking connection attempts from specified IP addresses. Furthermore, Cisco advise the use of certificate-based authentication in preference to credentials.

The attacks can be detected by examining System Logging (syslog) for an unusually high number of ASA syslog IDs outlined in the Cisco report.[9] The attacks resulted in hundreds of thousands or millions of rejected authentication attempts.

[8] Cisco warns of password-spraying attacks targeting VPN services, https://www.bleepingcomputer.com/news/security/cisco-warns-of-password-spraying-attacks-targeting-vpn-services/

[9] Best Practices Against Password Spray Attacks Impacting Remote Access VPN Services, https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/221806-password-spray-attacks-impacting-custome.html

MDR CYBER
Part of the Mishcon de Reya Group

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.

This document has been prepared for general guidance only, and does not constitute professional or legal advice. If you wish to receive legal advice we will need to provide you with a separate retainer letter and additional terms of business, as such work will be separately regulated by the Solicitors Regulation Authority (SRA).

You should not act upon the information contained in this publication without obtaining specific professional or legal advice.

Mishcon de Reya refers to Mishcon de Reya LLP which is a limited liability partnership, incorporated in England (number OC399969), whose registered office is at Africa House, 70 Kingsway, London WC2B 6AH. It is a body corporate which has members rather than Partners.

mishcon.com/cyber