FW: 【漏洞預警】XZ Utils存在高風險安全漏洞(CVE-2024-3094)，請儘速確認並進行修補！

1 封郵件

gz710@mail.ncku.edu.tw <gz710@mail.ncku.edu.tw> 2024年4月9日 下午4:27
收件者: nckucc_黃國展 <gz710@mail.ncku.edu.tw>
副本: nckucc_朱敏清 <kkinglord@mail.ncku.edu.tw>

各位老師好：

轉寄教育機構ANA通報平台通知，謝謝。

成大 計網中心 敬上

連絡電話 : 06-2757575轉61037

From: service <service@cert.tanet.edu.tw>
Sent: Tuesday, April 9, 2024 4:25 PM
To: service@cert.tanet.edu.tw
Subject: (ANA事件單通知:TACERT-ANA-2024040901044545)(【漏洞預警】XZ Utils存在高風險安全漏洞(CVE-2024-3094)，請儘速確認並進行修補！)

教育機構ANA通報平台

發佈編號	TACERT-ANA-2024040901044545	發佈時間	2024-04-09 16:01:46
事故類型	ANA-漏洞預警	發現時間	2024-04-09 13:11:46
影響等級	中		

[主旨說明:]【漏洞預警】XZ Utils存在高風險安全漏洞(CVE-2024-3094)，請儘速確認並進行修補！

[內容說明:]

轉發 國家資安資訊分享與分析中心 NISAC-200-202404-00000021

研究人員發現XZ Utils資料壓縮程式庫已遭受供應鏈攻擊(Supply Chain Attack)(CVE-2024-3094)，該程式之特定版本已被植入後門程式，並有部分Linux發行版本安裝受影響之XZ Utils版本，請儘速確認並依官方建議採取對應措施。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

- Alpine
- Fedora 41、Fedora Rawhide及Fedora Linux 40 beta
- Kali Linux
- openSUSE Tumbleweed與openSUSE MicroOS
- Debian
- XZ Utils 5.6.0與5.6.1

[建議措施:]

確認版本後，請配合官方說明確認是否需要更新或是降低XZ Utils版本：

- Alpine： https://security.alpinelinux.org/vuln/CVE-2024-3094
- Debian： https://security-tracker.debian.org/tracker/CVE-2024-3094
- Fedora： https://fedoramagazine.org/cve-2024-3094-security-alert-f40-rawhide/
- Kali Linux： https://www.kali.org/blog/about-the-xz-backdoor/
- openSUSE： https://news.opensuse.org/2024/03/29/xz-backdoor/

[參考資料:]
1. https://nvd.nist.gov/vuln/detail/CVE-2024-3094
2. https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know
3. https://unit42.paloaltonetworks.com/threat-brief-xz-utils-cve-2024-3094/
4. https://www.ithome.com.tw/news/162040
5. https://security.alpinelinux.org/vuln/CVE-2024-3094
6. https://security-tracker.debian.org/tracker/CVE-2024-3094
7. https://fedoramagazine.org/cve-2024-3094-security-alert-f40-rawhide/
8. https://www.kali.org/blog/about-the-xz-backdoor/
9. https://www.suse.com/security/cve/CVE-2024-3094.html
10. https://news.opensuse.org/2024/03/29/xz-backdoor/

(此通報僅在於告知相關資訊，並非為資安事件)，如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組
網址：https://info.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw