

張貼日期：2024/04/10

# 【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！

- 主旨說明：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。
- 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:
- 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/>

計算機與通訊中心  
網路系統組 敬啟

From:  
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:  
[https://net.nthu.edu.tw/netsys/mailling:announcement:20240410\\_02](https://net.nthu.edu.tw/netsys/mailling:announcement:20240410_02)

Last update: **2024/04/10 10:19**

