

教育機構ANA通報平台

發佈編號	TACERT-ANA-2025031209034646	發佈時間	2025-03-12 09:19:46
事故類型	ANA-漏洞預警	發現時間	2025-03-11 15:14:46
影響等級	低		

[主旨說明:]【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/03/03-2025/03/09)

[內容說明:]

轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202503-00000001

【CVE-2024-4885】Progress WhatsUp Gold Path Traversal Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Progress WhatsUp Gold存在路徑遍歷漏洞，允許未經身份驗證的攻擊者執行遠端程式碼。

【影響平台】請參考官方所列的影響版本

<https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024>

【CVE-2018-8639】Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability (CVSS v3.1: 7.8)

【是否遭勒索軟體利用:未知】 Microsoft Windows Win32k 存在不當資源關閉或釋放漏洞，允許本地經身份驗證的權限提升。成功利用此漏洞的攻擊者可以在核心模式下執行任意程式碼。

【影響平台】請參考官方所列的影響版本

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-8639>

【CVE-2022-43769】Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability (CVSS v3.1: 7.2)

【是否遭勒索軟體利用:未知】 Hitachi Vantara Pentaho BA Server存在特殊指令注入漏洞，允許攻擊者將Spring範本注入到屬性文件中，從而執行任意指令執行。

【影響平台】請參考官方所列的影響版本

<https://support.pentaho.com/hc/en-us/articles/14455561548301--Resolved-Pentaho-BA-Server-Failure-to-Sanitize-Special-Elements-into-a-Different-Plane-Special-Element-Injection-Versions-before-9-4-0-1-and-9-3-0-2-including-8-3-x-Impacted-CVE-2022-43769>

【CVE-2022-43939】Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Hitachi Vantara Pentaho BA Server存在非正規 URL 路徑授權漏洞，使攻擊者可以繞過授權檢查。

【影響平台】請參考官方所列的影響版本

<https://support.pentaho.com/hc/en-us/articles/14455394120333--Resolved-Pentaho-BA-Server-Use-of-Non-Canonical-URL-Paths-for-Authorization-Decisions-Versions-before-9-4-0-1-and-9-3-0-2-including-8-3-x-Impacted-CVE-2022-43939>

【CVE-2023-20118】Cisco Small Business RV Series Routers Command Injection Vulnerability (CVSS v3.1: 7.2)

【是否遭勒索軟體利用:未知】多款Cisco小型企業RV系列路由器存在網頁管理界面的指令注入漏洞。成功利用此漏洞的經身份驗證的遠端攻擊者可能獲得root權限並訪問未經授權的資料。

【影響平台】請參考官方所列的影響版本<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5>

【CVE-2025-22226】VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability (CVSS v3.1: 6.0)

【是否遭勒索軟體利用:未知】VMware ESXi、Workstation和Fusion存在資訊洩漏漏洞，該漏洞由HGFS的越界讀取導致。成功利用此漏洞可讓擁有虛擬機管理權限的攻擊者從VMX程序洩漏記憶體。

【影響平台】請參考官方所列的影響版本

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2025-22225】VMware ESXi Arbitrary Write Vulnerability (CVSS v3.1: 8.2)

【是否遭勒索軟體利用:未知】VMware ESXi存在任意寫入漏洞。成功利用此漏洞可讓擁有VMX程序權限的攻擊者觸發任意核心寫入，導致脫離沙箱。

【影響平台】請參考官方所列的影響版本

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2025-22224】VMware ESXi and Workstation TOCTOU Race Condition Vulnerability (CVSS v3.1: 8.2)

【是否遭勒索軟體利用:未知】VMware ESXi和Workstation存在TOCTOU競爭條件漏洞，可能導致越界寫入。成功利用此漏洞可讓具有本機管理權限的攻擊者以虛擬機的VMX程序在主機上執行程式碼。

【影響平台】請參考官方所列的影響版本

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2024-50302】Linux Kernel Use of Uninitialized Resource Vulnerability (CVSS v3.1: 5.5)

【是否遭勒索軟體利用:未知】Linux核心存在使用未初始化資源漏洞，允許攻擊者藉由特製的HID報告洩漏核心記憶體。

【影響平台】Linux 3.12至4.19.324(不含)的版本、Linux 4.2至5.4.286(不含)的版本、Linux 5.5至5.10.230(不含)的版本、Linux 5.11至5.15.172(不含)的版本、Linux 5.16至6.1.117(不含)的版本、Linux 6.2至6.6.61(不含)的版本、Linux 6.7至6.11.8(不含)的版本

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:]

詳細內容於內容說明欄之影響平台

[建議措施:]

【CVE-2024-4885】官方已針對漏洞釋出修復更新，請更新至相關版本

<https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024>

【CVE-2018-8639】官方已針對漏洞釋出修復更新，請更新至相關版本

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-8639>

【CVE-2022-43769】官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.pentaho.com/hc/en-us/articles/14455561548301--Resolved-Pentaho-BA-Server-Failure-to-Sanitize-Special-Elements-into-a-Different-Plane-Special-Element-Injection-Versions-before-9-4-0-1-and-9-3-0-2-including-8-3-x-Impacted-CVE-2022-43769>

【CVE-2022-43939】官方已針對漏洞釋出修復更新，請更新至相關版本

<https://support.pentaho.com/hc/en-us/articles/14455394120333--Resolved-Pentaho-BA-Server-Use-of-Non-Canonical-URL-Paths-for-Authorization-Decisions-Versions-before-9-4-0-1-and-9-3-0-2-including-8-3-x-Impacted-CVE-2022-43939>

【CVE-2023-20118】官方已針對漏洞釋出修復更新，請更新至相關版本 <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5>

【CVE-2025-22226】官方已針對漏洞釋出修復更新，請更新至相關版本 <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2025-22225】官方已針對漏洞釋出修復更新，請更新至相關版本 <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2025-22224】官方已針對漏洞釋出修復更新，請更新至相關版本 <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390>

【CVE-2024-50302】官方已針對漏洞釋出修復更新，請更新至相關版本

1. <https://git.kernel.org/stable/c/05ade5d4337867929e7ef664e7ac8e0c734f1aaf>
2. <https://git.kernel.org/stable/c/177f25d1292c7e16e1199b39c85480f7f8815552>
3. <https://git.kernel.org/stable/c/1884ab3d22536a5c14b17c78c2ce76d1734e8b0b>
4. <https://git.kernel.org/stable/c/3f9e88f2672c4635960570ee9741778d4135ecf5>
5. <https://git.kernel.org/stable/c/492015e6249fbc42138b49de3c588d826dd9648>

6. <https://git.kernel.org/stable/c/9d9f5c75c0c7f31766ec27d90f7a6ac673193191>
7. <https://git.kernel.org/stable/c/d7dc68d82ab3fcfc3f65322465da3d7031d4ab46>
8. <https://git.kernel.org/stable/c/e7ea60184e1e88a3c9e437b3265cbb6439aa7e26>

[參考資料:]

(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