教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026090409092424	發佈時間	2026-09-04 09:12:32
事故類型	ANA-漏洞預警	發現時間	2026-09-04 09:12:32
影響等級	中		

[主旨說明:]【漏洞預警】Splunk Enterprise 存在多項高風險安全漏洞，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 資安訊息警訊 NISAC-200-202609-00000006

研究人員發現 Splunk Enterprise 存在多項高風險安全漏洞(CVE-2026-76253、CVE-2026-76310 至 CVE-2026-76317、CVE-2026-76319、CVE-2026-76335 及 CVE-2026-76350 至 CVE-2026-76352)，其中最嚴重之 CVE-2026-76310 為不當存取控制(Improper Access Control)漏洞，未經身分鑑別之遠端攻擊者若持有嵌入式報表令牌(Token)，可下載相關搜尋工作的派送封存檔，並從中取得工作階段相關資訊，進而存取報表擁有者可存取之資料，並影響系統完整性。若報表擁有者具 admin 角色時，攻擊者甚至可執行管理作業，請儘速確認並進行修補。

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」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

Splunk Enterprise 9.4.0 至 9.4.13、10.0.0 至 10.0.8、10.2.0 至 10.2.5 及

10.4.0 至 10.4.1 版本

[建議措施:]

官方已針對漏洞釋出修補程式，請升級 Splunk Enterprise 至 9.4.14、10.0.9、10.26 或 10.4.2(含)以後版本。 詳細說明請參考官方公告，網址如下：

https://advisory.splunk.com/advisories/SVD-2026-0801

[參考資料:]

1. https://nvd.nist.gov/vuln/detail/CVE-2026-76253
2. https://nvd.nist.gov/vuln/detail/CVE-2026-76310
3. https://nvd.nist.gov/vuln/detail/CVE-2026-76311
4. https://nvd.nist.gov/vuln/detail/CVE-2026-76312
5. https://nvd.nist.gov/vuln/detail/CVE-2026-76313
6. https://nvd.nist.gov/vuln/detail/CVE-2026-76314
7. https://nvd.nist.gov/vuln/detail/CVE-2026-76315
8. https://nvd.nist.gov/vuln/detail/CVE-2026-76316
9. https://nvd.nist.gov/vuln/detail/CVE-2026-76317
10. https://nvd.nist.gov/vuln/detail/CVE-2026-76319
11. https://nvd.nist.gov/vuln/detail/CVE-2026-76335
12. https://nvd.nist.gov/vuln/detail/CVE-2026-76350
13. https://nvd.nist.gov/vuln/detail/CVE-2026-76351
14. https://nvd.nist.gov/vuln/detail/CVE-2026-76352
15. https://advisory.splunk.com/advisories/SVD-2026-0801