

【CVE-2026-20307】 已通過身分鑑別之遠端攻擊者可藉由向網頁管理介面傳送特製之 Java 序列化物件，於底層作業系統執行任意程式碼，並將權限提升至 root。

【CVE-2026-76423】 未經身分鑑別之遠端攻擊者可藉由向對外開放之 REST API 連接埠傳送特製 HTTP 請求，以管理者權限讀取及變更 ISE 組態與身分資料。

【CVE-2026-76460】 未經身分鑑別之遠端攻擊者可藉由向存在缺陷之 API 端點傳送特製請求，繞過網頁管理介面之身分鑑別，進而未授權存取受影響裝置。

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:]

Cisco ISE 與 ISE-PIC 3.1 至 3.5 版本

Cisco ISE 與 ISE-PIC 3.0(含)以前版本(已終止軟體維護)

[建議措施:]

官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下：

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ>

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ>

[ry/cisco-sa-ise-rce-se7bYU57](https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57)

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>

[参考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-20130>

2. <https://nvd.nist.gov/vuln/detail/CVE-2026-20192>

3. <https://nvd.nist.gov/vuln/detail/CVE-2026-20307>

4. <https://nvd.nist.gov/vuln/detail/CVE-2026-76423>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-76460>

6.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>

7.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ>

8.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57>

9.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>

10.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-jfxK98ZP>