

狀態:	Resolved-解決	開始日期:	2025-12-12
優先權:	High	完成日期:	
被分派者:	益利 周	完成百分比:	100%
分類:		預估工時:	0:00 小時
版本:		耗用工時:	2:00 小時
需求部門單位:		希望完成日期:	
聯絡人分機/手機:		實際提出日期:	
聯絡人e-mail:		實際完成日期:	

概述
Summary
An Improper Verification of Cryptographic Signature vulnerability [CWE-347] in FortiOS, FortiWeb, FortiProxy and FortiSwitchManager may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML message, if that feature is enabled on the device. Please note that the FortiCloud SSO login feature is not enabled in default factory settings. However, when an administrator registers the device to FortiCare from the device's GUI, unless the administrator disables the toggle switch "Allow administrative login using FortiCloud SSO" in the registration page, FortiCloud SSO login is enabled upon registration. To prevent being affected by this vulnerability on vulnerable versions, please turn off the FortiCloud login feature (if enabled) temporarily until upgrading to a non-affected version. To turn off FortiCloud login, go to System -> Settings -> Switch "Allow administrative login using FortiCloud SSO" to Off. Or type the following command in the CLI: <pre>config system global set admin-forticloud-sso-login disable end</pre>

Version	Affected	Solution
FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
FortiOS 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiOS 7.0	7.0.0 through 7.0.17	Upgrade to 7.0.18 or above
FortiOS 6.4	Not affected	Not Applicable
FortiProxy 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiProxy 7.4	7.4.0 through 7.4.10	Upgrade to 7.4.11 or above
FortiProxy 7.2	7.2.0 through 7.2.14	Upgrade to 7.2.15 or above
FortiProxy 7.0	7.0.0 through 7.0.21	Upgrade to 7.0.22 or above
FortiSwitchManager 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiSwitchManager 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above
FortiWeb 8.0	8.0.0	Upgrade to 8.0.1 or above
FortiWeb 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
FortiWeb 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiWeb 7.2	Not affected	Not Applicable
FortiWeb 7.0	Not affected	Not Applicable
Follow the recommended upgrade path using our tool at: https://docs.fortinet.com/upgrade-tool		

歷史

- #1 - 2025-12-12 14:58 - 益利 周
- 狀態 從 New-新增 變更為 In process-進行中
 - 被分派者 設定為 益利 周
 - 優先權 從 Normal 變更為 High
 - 完成百分比 從 0 變更為 10

已著手規劃 進行升級測試 新版本是否對目前環境造成影響.
安裝新版本後 運行測試兩周.觀察影響.
若未有顯著影響,續排定各點更新事宜.

- #2 - 2025-12-17 10:15 - 益利 周
- 檔案 clipboard-202512171002-kpivr.png 已新增
 - 狀態 從 In process-進行中 變更為 Resolved-解決
 - 完成百分比 從 10 變更為 100

clipboard-202512171002-9stwt.png

因 企業內 未使用 FortiCloud SSO 服務 不受影響. 暫緩升級 維持在 版本 7.4.7

同時選擇測試點 測試升級至新版本 7.4.9 對整體運作是否造成影響,預做升級測試.(目前已將洊止升級 7.4.9 觀察中)

檔案

clipboard-202512121453-bnevg.png	120 KB	2025-12-12	益利 周
----------------------------------	--------	------------	------

