مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in FortiSwitch Products

Tracking #:432317054

Date:09-04-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has disclosed a critical security vulnerability affecting multiple versions of its FortiSwitch product line.

TECHNICAL DETAILS:

Fortinet has disclosed a critical security vulnerability affecting multiple versions of its FortiSwitch product line. The flaw, tracked as CVE-2024-48887 and rated CVSS 9.3 (Critical), resides in the Graphical User Interface (GUI) and could allow remote, unauthenticated attackers to change administrative passwords without verification. Successful exploitation of this vulnerability may result in unauthorized administrative access, potentially leading to full control over the affected network switch infrastructure.

Organizations using vulnerable FortiSwitch versions are strongly advised to upgrade immediately to the fixed firmware versions released by Fortinet. Until patching is completed, mitigation measures such as disabling HTTP/HTTPS GUI access and restricting management access should be implemented.

Technical Details

- CVE ID: CVE-2024-48887
- Severity: Critical
- CVSS v3.1 Score: 9.3
- CWE Reference: CWE-620 (Unverified Password Change)
- Attack Vector: Remote
- Authentication Required: No
- Impact: Unauthorized password change → administrative access → full device compromise

Version	Affected	Solution
FortiSwitch 7.6	7.6.0	Upgrade to 7.6.1 or above
FortiSwitch 7.4	7.4.0 through 7.4.4	Upgrade to 7.4.5 or above
FortiSwitch 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiSwitch 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above
FortiSwitch 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above

Mitigation Steps (If Immediate Patching is Not Possible)

- **Disable GUI Access (HTTP/HTTPS):** Prevent access to the FortiSwitch GUI by disabling HTTP and HTTPS administrative interfaces.
- **Use Trusted Hosts:** Configure the trusted hosts feature to **restrict access to only known, secure IP addresses**.
- **Monitor for Suspicious Password Changes:** Review logs for abnormal or unauthorized password change activity.
- **Segment Management Network:** Ensure that management interfaces are isolated from untrusted networks.

RECOMMENDATIONS:

- Upgrade to Fixed Versions or Implement Workarounds, If Immediate Patching is Not Possible
- Regularly review system logs for suspicious activity, such as unauthorized password changes or failed login attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-435