EnCyb

Severity: High

Advisory Type: Security

Active Exploitation of FortiOS SSL VPN 2FA Bypass

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Active exploitation of a FortiOS SSL VPN vulnerability enables attackers to bypass 2FA and gain unauthorized access to affected systems. Organizations using impacted FortiOS versions are at increased risk of credential abuse, lateral movement, and compromise of critical network resources.

- CVE ID: CVE-2020-12812
- Active Region: Global
- Affected Sector: Any sector using FortiGate VPN infrastructure
- Affected Product: FortiOS SSL VPN
- Severity: High
- Published Date: December 25, 2025

AFFECTED VERSIONS

- FortiOS **6.0.9 and earlier**
- FortiOS **6.2.0 through 6.2.3**
- FortiOS **6.4.0**

FIXED VERSIONS

- FortiOS 6.0.10 or later
- FortiOS 6.2.4 or later
- FortiOS 6.4.1 or later

TECHNICAL DETAILS

- Target: FortiGate firewall appliances configured with SSL VPN access where local user accounts are integrated with LDAP-based authentication, commonly used for centralized identity management and group-based access control with two-factor authentication enabled.

- Root Cause: The vulnerability is caused by inconsistent username case handling between FortiGate's local authentication mechanism and external LDAP authentication. FortiGate treats local usernames as case-sensitive, while LDAP treats them as case-insensitive, allowing authentication to bypass configured two-factor authentication when the username casing does not exactly match the local account.

- Prerequistic For Exploitation: Exploitation requires a FortiGate SSL VPN setup using local users with LDAP authentication and 2FA enabled. An attacker with valid LDAP credentials can bypass 2FA by logging in with altered username casing, causing authentication to fall back to LDAP.

IMPACT

- Unauthorized access to VPN or administrative interfaces.
- Bypass of two-factor authentication controls.
- Increased risk of credential-based attacks and account compromise.
- Potential lateral movement within the internal network.
- Exposure of sensitive systems and data.
- Elevated risk of full network compromise if exploited by advanced threat actors.

RECOMMENDATIONS

- Upgrade FortiOS to a fixed version (6.0.10+, 6.2.4+, or 6.4.1+) to eliminate the vulnerability.
- Ensure username case sensitivity is properly configured by disabling case-sensitive matching where applicable.
- Review and remove unnecessary LDAP group mappings, especially those linked to VPN or administrative access.
- Enforce strict multi-factor authentication policies and validate that 2FA is correctly applied to all authentication paths.
- Audit authentication logs for signs of anomalous or unauthorized access attempts.
- Reset credentials for accounts that may have been exposed or misused.
- Check FortiCare settings to ensure FortiCloud SSO was not auto-enabled.

REFRENCE

- https://thehackernews.com/2025/12/fortinet-warns-of-active-exploitation.html
- https://www.fortinet.com/blog/psirt-blogs/product-security-advisory-and-analysis-observed-abuse-of-fg-ir-19-283

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com www.encyb.com