مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

FortiGate LDAP Misconfiguration Allowing Two-Factor Authentication Bypass

Tracking #:432318175

Date:25-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Fortinet has reported active exploitation of a previously disclosed vulnerability, FG-IR-19-283 (CVE-2020-12812), affecting FortiGate devices running specific LDAP and two-factor authentication (2FA) configurations.

TECHNICAL DETAILS:

Fortinet has observed active exploitation of a previously disclosed vulnerability, FG-IR-19-283 (CVE-2020-12812), affecting FortiGate devices running specific LDAP and two-factor authentication (2FA) configurations. The vulnerability allows LDAP-authenticated users to bypass two-factor authentication (2FA) by exploiting case-sensitivity mismatches between FortiGate and LDAP directory services. When exploited, attackers can authenticate successfully using valid LDAP credentials without triggering 2FA, potentially granting unauthorized access to administrative interfaces or VPN services.
Organizations running FortiOS versions prior to the fixed releases or with misconfigured LDAP group policies are at elevated risk. Successful exploitation should be treated as a security compromise, requiring immediate remediation and credential resets.

Technical Details
Vulnerability Overview

- **Identifier:** FG-IR-19-283 / CVE-2020-12812
- **Root Cause:**
  FortiGate treats usernames as **case-sensitive by default**, while most LDAP directories (e.g., Active Directory) treat usernames as **case-insensitive**.
- **Impact:**
  Authentication can fall back to LDAP group authentication when local user matching fails, allowing **2FA bypass**.

Affected Configuration Prerequisites
The vulnerability can be triggered **only if all of the following conditions exist**:

1. **Local FortiGate user accounts** are configured with **2FA enabled** and reference an LDAP directory.
2. The same users exist in **LDAP/Active Directory groups**.
3. At least one LDAP group (e.g., *Domain Users*, *Helpdesk*) is:
   - Configured on the FortiGate
   - Used in an authentication policy (Admin access, SSL VPN, or IPsec VPN)
4. Username case sensitivity remains **enabled** (default behavior in older FortiOS versions).

Mitigations
1. Mandatory Configuration Change (Immediate)

- **For FortiOS 6.0.10 / 6.2.4 / 6.4.1 and earlier syntax:**
  set username-case-sensitivity disable
- **For FortiOS 6.0.13 / 6.2.10 / 6.4.7 / 7.0.1 and above:**
  set username-sensitivity disable

Effect:
Ensures FortiGate treats all username case variations as identical, preventing authentication fallback to LDAP groups.

RECOMMENDATIONS:

- Organizations are strongly urged to:
  - Apply the recommended configuration immediately and apply mitigation if needed
  - Review LDAP authentication flows
  - Treat any successful bypass as a security incident

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://www.fortinet.com/blog/psirt-blogs/product-security-advisory-and-analysis-observed-abuse-of-fg-ir-19-283