CyberSOC Threat Notification

PAN-OS, GlobalProtect VPN Authentication Bypass Vulnerability

Executive Summary

On November 11th, Palo Alto released a security advisory detailing a high severity authentication bypass vulnerability in the GlobalProtect SSL VPN component of Palo Alto Networks PAN-OS software.

Description

The vulnerability could allow an attacker to bypass all client certificate checks with an invalid certificate. A remote attacker could leverage this flaw to successfully authenticate as any user and gain access to restricted VPN network resources when the gateway or portal is configured to rely entirely on certificate-based authentication. This issue is only applicable to PAN-OS appliances using the GlobalProtect SSL VPN gateway or portal configured to allow users to authenticate with client certificate authentication. This issue cannot be exploited if client certificate authentication is not in use. According to Palo Alto, no evidence of active exploitation has been identified at this time.

Affected Products

- PAN-OS Versions:
  - 10.0 versions earlier than 10.0.1
  - 9.1 versions earlier than 9.1.5
  - 9.0 versions earlier than 9.0.11
  - 8.1 versions earlier than 8.1.17

Safeguards/Recommendations

Affected customers are strongly encouraged to upgrade to a fixed version. The issue can also be mitigated by configuring GlobalProtect SSL VPN to require gateway and portal users to authenticate with their credentials.

Vendor: Palo Alto

CVE-ID: CVE-2020-2050

Published: Nov 11, 2020

CVSS V3 Overall score: 8.2

Criticality: High

Patch Availability: Yes

Vulnerability Type: Improper Authorization

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Unchanged

Confidentiality: High

Integrity: Low

Availability: None

Confidence Metrics

Exploitability: Unproven

Remediation Level: Official Fix

Report Confidence: Confirmed

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io