مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Palo Alto Networks GlobalProtect

Tracking #:432316557

Date:26-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in GlobalProtect app that could enable attackers to install malware, steal data, or compromise systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2024-5921
- CVSS Score 5.6 Medium
- Palo Alto Networks has identified a vulnerability in its GlobalProtect app. This vulnerability is due to insufficient certificate validation, which allows attackers to connect the GlobalProtect app to arbitrary servers. This can enable the installation of malicious root certificates on endpoints, potentially leading to the installation of malicious software signed by these certificates.
- This vulnerability poses a significant security risk as it could allow attackers to gain complete control over endpoints by installing malicious software.

Affected Versions:

- **Windows**: All versions of 6.3, 6.1, 6.0, 5.1, and GlobalProtect UWP App.
- **macOS and Linux**: All versions of 6.2.
- **Windows (specific to version 6.2)**: Versions prior to 6.2.6.

Fixed Versions:

- GlobalProtect app version 6.2.6 and later versions on Windows

Mitigations for other affected versions:

- Using the GlobalProtect app in FIPS-CC mode.
- Installing GlobalProtect with specific parameters to enforce strict certificate validation:
  - msiexec.exe /i GlobalProtect64.msi FULLCHAINCERTVERIFY="yes"

  To specify the certificate store and location:
  - msiexec.exe /i GlobalProtect64.msi FULLCHAINCERTVERIFY="yes" CERTSTORE="machine" CERTLOCATION="ROOT"
- **CERTSTORE options**: "machine" (recommended) or "user".
- **CERTLOCATION options**: "ROOT" (recommended), "MY," "trusted publisher," "ca," "truest," "authroot," "smartcardroot," and "userds"

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Palo Alto Networks.

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://security.paloaltonetworks.com/CVE-2024-5921