مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in WatchGuard and Panda

Tracking #:432316494

Date:11-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity Vulnerability in WatchGuard EPDR, Panda AD360 and Panda Dome on Windows that could potentially be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2024-8424
- CVSS Score 7.8 High
- An improper privilege management vulnerability exists in WatchGuard EPDR, Panda AD360, and Panda Dome products for Windows. This improper privilege management flaw in the PSANHost.exe module allows an authenticated attacker with local access to delete arbitrary files with SYSTEM permissions, potentially leading to severe system compromise.
- Successful exploitation of this vulnerability could allow an attacker to delete critical system files, compromise system integrity, potentially achieve further privilege escalation, and cause denial of service conditions.

Affected Products and Versions:

- WatchGuard EPDR: Versions prior to 8.00.23.0000
- Panda AD360: Versions prior to 8.00.23.0000
- Panda Dome: Versions prior to 22.03.00

Fixed Versions:

- WatchGuard EPDR: Version 8.00.23.0000 or later
- Panda AD360: Version 8.00.23.0000 or later
- Panda Dome: Version 22.03.00 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00017