SSA-455250: Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 devices before V11.1.2-h3

Publication Date: 2024-04-09
Last Update: 2024-07-09
Current Version: V1.2
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 5.1

SUMMARY

Palo Alto Networks has published [1] information on vulnerabilities in PAN-OS. This advisory lists the related Siemens Industrial products affected by these vulnerabilities.

Siemens has released a new version of Palo Alto Networks Virtual NGFW for RUGGEDCOM APE1808 and recommends to update to the latest version. Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications.

[1] https://security.paloaltonetworks.com/

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM APE1808:	Upgrade Palo Alto Networks Virtual NGFW V11.1.2-h3. Contact customer support to receive patch and update information
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW before V11.1.2-h3 affected by CVE-2017-8923, CVE-2017-9120, CVE-2020-25658, CVE-2021-21708, CVE-2021-43527, CVE-2022-1271, CVE-2022-3515, CVE-2022-31676, CVE-2022-37454, CVE-2022-47629, CVE-2023-0286, CVE-2023-6789, CVE-2023-6793, CVE-2024-0008, CVE-2024-3383, CVE-2024-3386, CVE-2024-3387, CVE-2024-3388	Upgrade Palo Alto Networks Virtual NGFW V11.1.2-h3. Contact customer support to receive patch and update information
RUGGEDCOM APE1808: All versions with Palo Alto Networks Virtual NGFW before V11.1.2-h3 that are configured with BGP routing features enabled affected by CVE-2023-38802	Upgrade Palo Alto Networks Virtual NGFW V11.1.2-h3. Contact customer support to receive patch and update information

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The RUGGEDCOM APE1808 is a powerful utility-grade application hosting platform that lets you deploy a range of commercially available applications for edge computing and cybersecurity in harsh, industrial environments.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2017-8923

The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2017-9120

PHP 7.x through 7.1.5 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a long string because of an Integer overflow in mysqli_real_escape_string.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2020-25658

It was found that python-rsa is vulnerable to Bleichenbacher timing attacks. An attacker can use this flaw via the RSA decryption API to decrypt parts of the cipher text encrypted with RSA.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-385: Covert Timing Channel

Vulnerability CVE-2021-21708

In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-43527

NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. Note: This vulnerability does NOT impact Mozilla Firefox. However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-1271

An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-3515

A vulnerability was found in the Libksba library due to an integer overflow within the CRL parser. The vulnerability can be exploited remotely for code execution on the target system by passing specially crafted data to the application, for example, a malicious S/MIME attachment.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-31676

VMware Tools (12.0.0, 11.x.y and 10.x.y) contains a local privilege escalation vulnerability. A malicious actor with local non-administrative access to the Guest OS can escalate privileges as a root user in the virtual machine.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2022-37454

The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-47629

Libksba before 1.6.3 is prone to an integer overflow vulnerability in the CRL signature parser.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2023-0286

There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-6789

A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a malicious authenticated read-write administrator to store a JavaScript payload using the web interface. Then, when viewed by a properly authenticated administrator, the JavaScript payload executes and disguises all associated actions as performed by that unsuspecting authenticated administrator.

CVSS v3.1 Base Score	4.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2023-6793

An improper privilege management vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to revoke active XML API keys from the firewall and disrupt XML API usage.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-269: Improper Privilege Management

Vulnerability CVE-2023-38802

FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted BGP update with a corrupted attribute 23 (Tunnel Encapsulation).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.2
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Product Specific Vulnerability Description

For the following products, the impact of the vulnerability is different.

RUGGEDCOM APE1808:

FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted BGP update with a corrupted attribute 23 (Tunnel Encapsulation)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C (7.5)

Vulnerability CVE-2024-0008

Web sessions in the management interface in Palo Alto Networks PAN-OS software do not expire in certain situations, making it susceptible to unauthorized access.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

Vulnerability CVE-2024-3383

A vulnerability in how Palo Alto Networks PAN-OS software processes data received from Cloud Identity Engine (CIE) agents enables modification of User-ID groups. This impacts user access to network resources where users may be inappropriately denied or allowed access to resources based on your existing Security Policy rules.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H
CWE	CWE-282: Improper Ownership Management

Vulnerability CVE-2024-3386

An incorrect string comparison vulnerability in Palo Alto Networks PAN-OS software prevents Predefined Decryption Exclusions from functioning as intended. This can cause traffic destined for domains that are not specified in Predefined Decryption Exclusions to be unintentionally excluded from decryption.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CWE	CWE-436: Interpretation Conflict

Vulnerability CVE-2024-3387

A weak (low bit strength) device certificate in Palo Alto Networks Panorama software enables an attacker to perform a meddler-in-the-middle (MitM) attack to capture encrypted traffic between the Panorama management server and the firewalls it manages. With sufficient computing resources, the attacker could break encrypted communication and expose sensitive information that is shared between the management server and the firewalls.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2024-3388

A vulnerability in the GlobalProtect Gateway in Palo Alto Networks PAN-OS software enables an authenticated attacker to impersonate another user and send network packets to internal assets. However, this vulnerability does not allow the attacker to receive response packets from those internal assets.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N
CWE	CWE-269: Improper Privilege Management

ADDITIONAL INFORMATION

Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications [1]. PANW provides a public RSS feed for their security alerts to which customers can also subscribe [2].

PANW has issued and Informational Bulletin [3] advising on CVE-2017-8923, CVE-2017-9120, CVE-2020-25658, CVE-2021-21708, CVE-2021-43527, CVE-2022-1271, CVE-2022-3515, CVE-2022-31676, CVE-2022-37454, CVE-2022-47629, CVE-2023-0286. PANW evaluation has not determined sigificant impact of the aforementioned CVEs on PAN-OS.

[1] https://security.paloaltonetworks.com/?version=11.0.1&product=PAN-OS
[2] https://security.paloaltonetworks.com/rss.xml
[3] https://security.paloaltonetworks.com/PAN-SA-2024-0004

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-04-09):	Publication Date
V1.1 (2024-05-14):	Added newly published upstream vulnerabilities: CVE-2017-8923, CVE-2017-9120, CVE-2020-25658, CVE-2021-21708, CVE-2021-43527, CVE-2022-1271, CVE-2022-31676, CVE-2022-3515, CVE-2022-37454, CVE-2022-47629, CVE-2023-0286, CVE-2024-3383, CVE-2024-3386, CVE-2024-3387, CVE-2024-3388, CVE-2024-3400
V1.2 (2024-07-09):	Added fix for RUGGEDCOM APE1808 devices configured with Palo Alto Networks Virtual NGFW. Moved CVE-2023-48795 to SSA-364175

TERMS OF USE