

CVE-2020-2021

Palo Alto Networks PAN-OS Authentication Bypass Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Ransomware use known

When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability.

EVRS 85/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.044 91.2nd percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.044 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

This issue affects PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL). This issue does not affect PAN-OS 7.1. This issue cannot be exploited if SAML is not used for authentication. This issue cannot be exploited if the 'Validate Identity Provider Certificate' option is enabled (checked) in the SAML Identity Provider Server Profile. Resources that can be protected by SAML-based single sign-on (SSO) authentication are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN, Authentication and Captive Portal, PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces, Prisma Access. In the case of GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal, and Prisma Access, an unauthenticated attacker with network access to the affected servers can gain access to protected resources if allowed by configured authentication and Security policies. There is no impact on the integrity and availability of the gateway, portal or VPN server. An attacker cannot inspect or tamper with sessions of regular users. In the worst case, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N). In the case of PAN-OS and Panorama web interfaces, this issue allows an unauthenticated attacker with network access to the PAN-OS or Panorama web interfaces to log in as an administrator and perform administrative actions. In the worst-case scenario, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). If the web interfaces are only accessible to a restricted management network, then the issue is lowered to a CVSS Base Score of 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
pan-os	$\geq 8.0.0 \leq 8.0.20$ $\geq 8.1.0 < 8.1.15$ $\geq 9.0.0 < 9.0.9$ $\geq 9.1.0 < 9.1.3$	after 8.0.20 · 8.1.15 · 9.0.9 · 9.1.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-84wc-9427-hw23
NVD nvd.nist.gov/vuln/detail/CVE-2020-2021

Additional guidance security.paloaltonetworks.com/CVE-2020-2021
CISA KEY cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-22049

Current data evulnable.com/vulnerability-management/cve/CVE-2020-2021

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.