



CVE-2020-2041

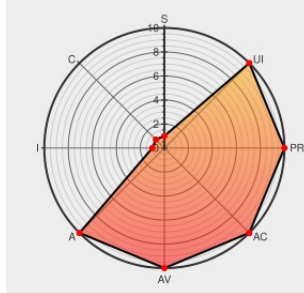
Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:08 PM UTC

CVE-2020-2041

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Pan-os](#) from [Paloaltonetworks](#) contain the following vulnerability:

An insecure configuration of the appweb daemon of Palo Alto Networks PAN-OS 8.1 allows a remote unauthenticated user to send a specifically crafted request to the device that causes the appweb service to crash. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts all versions of PAN-OS 8.0, and PAN-OS 8.1 versions earlier than 8.1.16.

CVE-2020-2041 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability.

Vulnerability Patch/Work Around

This issue impacts the management web interface of PAN-OS. You can mitigate the impact of this issue by following best practices for securing the PAN-OS management web interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at <https://docs.paloaltonetworks.com/best-practices>.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

NONE NONE COMPLETE

Description	Tags	Link
-------------	------	------

CVE-2020-2041 PAN-OS: Management web interface denial-of-service (DoS)	Vendor Advisory security.paloaltonetworks.com text/html	 MISC security.paloaltonetworks.com/CVE-2020-2041
--	---	---

[illegible]

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

```
cpe:2.3:o:paloaltonetworks:pan-os:*.~::~:
```

Period	Costs	Revenue	Profit
1990-1999	100	100	0
2000-2009	100	100	0
2010-2019	100	100	0
2020-2029	100	100	0
2030-2039	100	100	0
2040-2049	100	100	0
2050-2059	100	100	0
2060-2069	100	100	0
2070-2079	100	100	0
2080-2089	100	100	0
2090-2099	100	100	0
2100-2109	100	100	0
2110-2119	100	100	0
2120-2129	100	100	0
2130-2139	100	100	0
2140-2149	100	100	0
2150-2159	100	100	0
2160-2169	100	100	0
2170-2179	100	100	0
2180-2189	100	100	0
2190-2199	100	100	0
2200-2209	100	100	0
2210-2219	100	100	0
2220-2229	100	100	0
2230-2239	100	100	0
2240-2249	100	100	0
2250-2259	100	100	0
2260-2269	100	100	0
2270-2279	100	100	0
2280-2289	100	100	0
2290-2299	100	100	0
2300-2309	100	100	0
2310-2319	100	100	0
2320-2329	100	100	0
2330-2339	100	100	0
2340-2349	100	100	0
2350-2359	100	100	0
2360-2369	100	100	0
2370-2379	100	100	0
2380-2389	100	100	0
2390-2399	100	100	0
2400-2409	100	100	0
2410-2419	100	100	0
2420-2429	100	100	0
2430-2439	100	100	0
2440-2449	100	100	0
2450-2459	100	100	0
2460-2469	100	100	0
2470-2479	100	100	0
2480-2489	100	100	0
2490-2499	100	100	0
2500-2509	100	100	0
2510-2519	100	100	0
2520-2529	100	100	0
2530-2539	100	100	0
2540-2549	100	100	0
2550-2559	100	100	0
2560-2569	100	100	0
2570-2579	100	100	0
2580-2589	100	100	0
2590-2599	100	100	0
2600-2609	100	100	0
2610-2619	100	100	0
2620-2629	100	100	0
2630-2639	100	100	0
2640-2649	100	100	0
2650-2659	100	100	0
2660-2669	100	100	0
2670-2679	100	100	0
2680-2689	100	100	0
2690-2699	100	100	0
2700-2709	100	100	0
2710-2719	100	100	0
2720-2729	100	100	0
2730-2739	100	100	0
2740-2749	100	100	0
2750-2759	100	100	0
2760-2769	100	100	0
2770-2779	100	100	0
2780-2789	100	100	0
2790-2799	100	100	0
2800-2809	100	100	0
2810-2819	100	100	0
2820-2829	100	100	0
2830-2839	100	100	0
2840-2849	100	100	0

This issue was found by Nicholas Newsom of Palo Alto Networks during internal security

Next ID→

CVE.report and Source URL Uptime Status status.cve.report