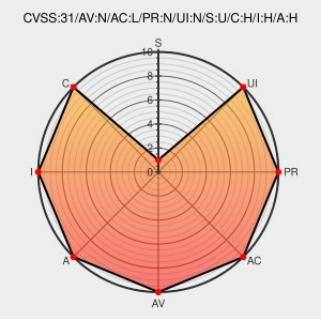
CVE-2021-42756

Published on: Not Yet Published

Last Modified on: 02/24/2023 07:58:00 PM UTC

CVE-2021-42756

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fortiweb from Fortinet contain the following vulnerability:

Multiple stack-based buffer overflow vulnerabilities [CWE-121] in the proxy daemon of FortiWeb 5.x all versions, 6.0.7 and below, 6.1.2 and below, 6.2.6 and below, 6.3.16 and below, 6.4 all versions may allow an unauthenticated remote attacker to achieve arbitrary code execution via specifically crafted HTTP requests.

CVE-2021-42756 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
PSIRT Advisories | FortiGuard	fortiguard.com text/html	MISC fortiguard.com/psirt/FG-IR-21-186

Related QID Numbers

730730 Fortinet - FortiNAC and FortiWeb Multiple Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortiweb	All	All	All	All
Application	Fortinet	Fortiweb	All	All	All	All

cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*:

cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-42756 : Multiple stack-based buffer overflow vulnerabilities [CWE-121] in the proxy daemon of FortiWeb 5.x… twitter.com/i/web/status/1…	2023-02-16 19:19:39
/r/netcve	CVE-2021-42756	2023-02-16 19:38:40
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY – Multiple Vulnerabilities in FortiWeb could allow for Arbitrary Code Execution – PATCH: NOW	2023-02-17 18:51:35
/r/u/BP_APG	Fortinet Released Patches for 40 Vulnerabilities Affecting Multiple Software Solutions	2023-02-20 22:17:35

← Previous ID

Next ID→