



CVE-2020-12812

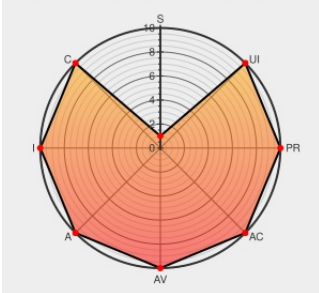
Published on: 07/24/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-12812

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

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



Certain versions of [Fortios](#) from [Fortinet](#) contain the following vulnerability:

An improper authentication vulnerability in SSL VPN in FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9 and below may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.

CVE-2020-12812 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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
FortiOS SSL VPN 2FA bypass by changing username case FortiGuard	Vendor Advisory fortiguard.com text/html	MISC fortiguard.com/psirt/FG-IR-19-283

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	6.4.0	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	6.4.0	All	All	All
cpe:2.3:o:fortinet:fortios:*****:						
cpe:2.3:o:fortinet:fortios:6.4.0:*****:						
cpe:2.3:o:fortinet:fortios:*****:						
cpe:2.3:o:fortinet:fortios:6.4.0:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LindseyOD123	APT actors are actively exploiting known #Fortinet FortiOS flaws CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591,... twitter.com/i/web/status/1...	2021-04-02 16:57:45
 @aidaakl	MT @LindseyOD123 APT actors are actively exploiting known #Fortinet FortiOS flaws CVE-2018-13379, CVE-2020-12812, a... twitter.com/i/web/status/1...	2021-04-02 16:59:52
 @campuscodi	The three FortiOS vulnerabilities are: -CVE 2018-13379 (because obviously) -CVE-2020-12812 ? -CVE-2019-5591 ? https://t.co/aFptwHBbXR	2021-04-02 17:16:42
 @hiramcoop	FBI and CISA warn of state hackers attacking Fortinet FortiOS servers CVE-2018-13379, CVE-2020-12812, CVE-2019-5591. bleepingcomputer.com/news/security/...	2021-04-02 19:13:10
 @ItsKarl0z	@CISAgov @FBI vulnerabilities CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591	2021-04-02 19:34:53
 @ipssignatures	I know no IPS that has a protection/signature/rule for the vulnerability CVE-2020-12812. The vuln was published 251... twitter.com/i/web/status/1...	2021-04-02 23:04:01
 @ipssignatures	The vuln CVE-2020-12812 has a tweet created 0 days ago and retweeted 7 times. twitter.com/campuscodi/sta... #S623logqvvec	2021-04-02 23:04:01
 @holisticinfosec	APT actors actively exploiting known Fortinet FortiOS vulns CVE-2018-13379, CVE-2020-12812, & CVE-2019-5591. May us... twitter.com/i/web/status/1...	2021-04-03 02:26:37

✖ @ipssignatures	The vuln CVE-2020-12812 has a tweet created 0 days ago and retweeted 10 times. twitter.com/campuscodi/sta... #pow1rtrtwwcve	2021-04-03 03:06:00
✖ @Har_sia	CVE-2020-12812 har-sia.info/CVE-2020-12812... #HarsialInfo	2021-04-03 18:24:02
✖ @twelvesec	#Hackers are using 3 #cybersecurity #vulnerabilities (CVE-2018-13379, CVE-2019-5591, CVE-2020-12812) found in the F... twitter.com/i/web/status/1...	2021-04-05 13:44:02
✖ @Attackerkb_Bot	A new #attackerkb assesment on 'CVE-2020-12812' has been created by ccondon-r7. Attacker Value: 0 Exploitability:... twitter.com/i/web/status/1...	2021-04-05 14:09:37
✖ @vFeed_IO	@FBI & the @CISAgov warn about APT Actors Exploit FortiOS Vulnerabilities (CVE-2018-13379, CVE-2020-12812 and CVE-... twitter.com/i/web/status/1...	2021-04-05 15:48:03
✖ @ToolsWatch	@FBI & @CISAgov warn about APT Actors Exploit FortiOS Vulnerabilities (CVE-2018-13379, CVE-2020-12812 and CVE-2019-... twitter.com/i/web/status/1...	2021-04-05 15:48:27
✖ @onuroktay	FBI, Rus ve Çin'li hackerlerin FortiGate'in CVE-2018-13379, CVE-2019-5591 and CVE-2020-12812 açıklıklarını kullanar... twitter.com/i/web/status/1...	2021-04-06 05:29:52
✖ @cert_ist	La CISA et le FBI nous informent que des APT exploitent activement les CVE-2018-13379, CVE-2020-12812 et CVE-2019-5... twitter.com/i/web/status/1...	2021-04-06 08:52:42
✖ @foxbook	FBIの4/2アラートです。CVE-2018-13379、CVE-2020-12812、CVE-2019-5591の脆弱性がAPT攻撃者（ランサムオペレータ）によって探されているとの内容です。「APT Actors Explo... twitter.com/i/web/status/1...	2021-04-08 20:27:59
✖ @_GrimSqueaker_	tenable.com/blog/cve-2018-... @TenableSecurity #TenableResearch	2021-04-08 22:23:16
✖ @ka0com	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors - tenable.com/blog/cve-2018-...	2021-04-08 23:13:04
✖ @Michal_Jarski	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors ow.ly/jbrS102FCac	2021-04-09 10:19:06
✖ @Art_Capella	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors ow.ly/gT6B102FEfE	2021-04-09 13:11:24
✖ @stuart_smiles	Fortinet patch advice from NCSC ncsc.gov.uk/news/critical-... Cve-2018-13379 cve-2020-12812 cve-2019-5591 Patch patch patch.	2021-04-09 15:09:31
✖ @Har_sia	CVE-2020-12812 har-sia.info/CVE-2020-12812... #HarsialInfo	2021-04-09 18:29:03
✖ @intrasecure	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors bit.ly/3tcWpB8	2021-04-12 19:15:01
✖ @dansantanna	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors ow.ly/IFRF102GrmQ	2021-04-13 01:05:03
✖ @AlicePintori	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors ow.ly/zJRm102I3se	2021-04-26 11:39:14
✖ @bishopfox	ICYMI: Three #CVEs affecting #Fortinet are again being targeted by attackers: CVE-2020-12812, CVE-2019-5591, and CV... twitter.com/i/web/status/1...	2021-05-09 23:54:59
✖ @c3rb3ru5d3d53c	CVE-2020-12812 and CVE-2019-5591 #exploits, no public #PoC, no detection in ETPro. And people wonder why they are g... twitter.com/i/web/status/1...	2021-05-27 18:15:38
✖ @uuallan	The vulnerabilities being exploited are tracked as CVE 2018-13379, CVE-2020-12812, and CVE-2019-5591. Note: none o... twitter.com/i/web/status/1...	2021-05-27 19:08:19
✖ @ipssignatures	The vuln CVE-2020-12812 has a tweet created 0 days ago and retweeted 11 times. twitter.com/uuallan/status... #pow1rtrtwwcve	2021-05-27 23:06:00
✖ @M0teki	@GelosSnake 2FA bypass was also used heavily in several campaigns (CVE-2020-12812) after most organizations employed the CVE-2018-1337 patch	2021-05-28 10:16:07

 @KathleenRytman	CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591 are being exploited. Each of these vulnerabilities is known and p... twitter.com/i/web/status/1...	2021-05-28 21:17:54
 @HAL_CSIRT	【FBIが「フォーティネット製品の脆弱性を利用したハッカーが地方自治体のサーバーを侵害した」と発表】 ・ CVE-2018-13379 ・ CVE-2020-12812 ・ CVE-2019-5591 ・ 被害者の運用する内部ネットワーク... twitter.com/i/web/status/1...	2021-05-30 13:34:26
 @g_yotuya	CVE-2020-12812 FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9 CVE-2018-13379 FortiOS 6.0.0to6.0.4、5.6.3to5.6.7、5.4.6to5.4.12	2021-06-23 05:11:24
 @asharam_maskare	3. Fortinet FortiGate SSL VPN: CVE-2018-13379, CVE-2020-12812, CVE-2019-5591 #Fortinet	2021-11-11 05:31:52
 @catnap707	“2021年3月から「FortiOS」における既知の脆弱性（CVE-2018-13379、CVE-2020-12812、CVE-2019-5591）を、同年10月からはExchange Serverの脆弱性「ProxyShell」... twitter.com/i/web/status/1...	2021-11-19 00:19:57
 @housu_jp	CVE-2018-13379, CVE-2019-5591, CVE-2020-12812: Fortinet Vulnerabilities Targeted by APT Actors tenable.com/blog/cve-2018-...	2022-09-26 21:19:13
 @DiegoKoprivtza	Play se aprovecha de las vulnerabilidades del SSL VPN de FortiOS y FortiProxy: → →	2022-12-07 16:36:16
 /r/cybersecurity	[FBI/CISA] APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attack - FortiNet/FortiOS - scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591	2021-04-03 08:17:23
 /r/blueteamsec	[FBI/CISA] APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attack - FortiNet/FortiOS - scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591	2021-04-03 08:14:47
 /r/netsec	[FBI/CISA] APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attack - FortiNet/FortiOS - scanning devices on ports 4443, 8443, and 10443 for CVE-2018-13379, and enumerated devices for CVE-2020-12812 and CVE-2019-5591	2021-04-03 08:28:51
 /r/sysadmin	Update FortiOS as soon as possible: FBI, CISA warn Fortinet FortiOS vulnerabilities are being actively exploited -- APT groups are suspected of harnessing three bugs, two critical, for data exfiltration purposes.	2021-04-06 18:38:15
 /r/fortinet	CVE-2020-12812 only affect LDAP?	2021-04-07 21:59:00
 /r/u/CyberHoot	CISA's Top Vulnerabilities in 2020 and 2021 - CyberHoot	2021-08-03 16:45:38

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)