



Stack-based buffer overflow in command line interpreter

IR Number	FG-IR-21-132
Published Date	Feb 1, 2022
Severity	High
CVSSv3 Score	7.4
Impact	Execute unauthorized code or commands
CVE ID	CVE-2021-36193
Download	CVRF

Summary

Multiple stack-based buffer overflows [CWE-121] in the command line interpreter of FortiWeb,

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

Accept

FortiMail version 7.0.0 through 7.0.2
FortiMail version 6.4.0 through 6.4.6
FortiMail version 6.2.0 through 6.2.8
FortiMail 6.0 all versions
FortiMail 5.4 all versions
FortiVoiceEnterprise version 6.4.0 through 6.4.4
FortiVoiceEnterprise version 6.0.0 through 6.0.10
FortiDDoS-F version 6.3.0
FortiDDoS-F version 6.2.0 through 6.2.2
FortiDDoS-F version 6.1.0 through 6.1.4
FortiADC version 7.0.0
FortiADC version 6.2.0 through 6.2.2
FortiADC version 6.1.0 through 6.1.6
FortiADC 6.0 all versions
FortiADC 5.4 all versions
FortiADC 5.3 all versions
FortiADC 5.2 all versions
FortiADC 5.1 all versions
FortiADC 5.0 all versions
FortiNDR 1.5 all versions
FortiNDR 1.4 all versions
FortiNDR 1.3 all versions
FortiNDR 1.2 all versions
FortiNDR 1.1 all versions
FortiDDoS-CM version 5.5.0 through 5.5.1
FortiDDoS-CM version 5.4.0 through 5.4.3
FortiDDoS-CM version 5.3.0 through 5.3.1
FortiDDoS-CM 5.2 all versions
FortiDDoS-CM 5.1 all versions
FortiDDoS-CM 5.0 all versions
FortiDDoS-CM 4.7 all versions

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

FortiDDoS 5.2 all versions
FortiDDoS 5.1 all versions
FortiDDoS 5.0 all versions
FortiDDoS 4.7 all versions
FortiDDoS 4.6 all versions
FortiDDoS 4.5 all versions
FortiDDoS 4.4 all versions

Solutions

Please upgrade to FortiFone version 3.0.12 or above
Please upgrade to FortiWeb version 7.0.0 or above
Please upgrade to FortiWeb version 6.4.2 or above
Please upgrade to FortiWeb version 6.3.17 or above
Please upgrade to FortiWeb version 6.3.16 or above
Please upgrade to FortiWeb version 6.2.7 or above
Please upgrade to FortiRecorder version 7.0.0 or above
Please upgrade to FortiRecorder version 6.4.3 or above
Please upgrade to FortiRecorder version 6.0.11 or above
Please upgrade to FortiVoiceEnterprise version 6.4.5 or above
Please upgrade to FortiVoiceEnterprise version 6.0.11 or above
Please upgrade to FortiMail version 7.2.0 or above
Please upgrade to FortiMail version 7.0.3 or above
Please upgrade to FortiMail version 6.4.7 or above
Please upgrade to FortiMail version 6.2.9 or above
Please upgrade to FortiDDoS-F version 6.3.1 or above
Please upgrade to FortiDDoS-F version 6.2.3 or above
Please upgrade to FortiDDoS-F version 6.1.5 or above
Please upgrade to FortiADC version 7.0.1 or above

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).

Please upgrade to FortiDDoS-CM version 5.5.2 or above

Please upgrade to FortiDDoS-CM version 5.4.3 or above

Please upgrade to FortiDDoS-CM version 5.3.2 or above

Acknowledgement

Internally discovered and reported by Giuseppe Cocomazzi of Fortinet Product Security team.

Timeline

2022-02-01: Initial publication

FORTINET[®]

[Contact Us](#) | [Legal](#) | [Privacy](#) | [Partners](#) | [Feedback](#)



Copyright © 2026 Fortinet, Inc. All Rights Reserved.

This site uses cookies. Some are essential to the operation of the site; others help us improve the user experience. By continuing to use the site, you consent to the use of these cookies. To learn more about cookies, please read our [privacy policy](#).