



Authentication bypass in administrative interface

IR Number **FG-IR-22-377**

Published Date **Oct 10, 2022**

Component **GUI**

Severity ** Critical**

CVSSv3 Score **9.6**

Impact **Execute unauthorized code or commands**

CVE ID **CVE-2022-40684**

Download ** CVRF**

Language

English



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

device's logs:

```
user=Local_Process_Access
```

Please contact customer support for assistance.

UPDATE:

Fortinet is aware of instances where this vulnerability was exploited to download the config file from the targeted devices, and to add a malicious super_admin account called 'fortigate-tech-support':

```
# show system admin
edit fortigate-tech-support
set accprofile super_admin
set vdom root
set password ENC [...]
next
```

Please contact customer support for assistance.

Workaround:

FortiOS:

Disable HTTP/HTTPS administrative interface

OR

Limit IP addresses that can reach the administrative interface:

```
config firewall address
edit my_allowed_addresses
set subnet <MY IP> <MY SUBNET>
end
```

Then create an Address Group:

```
config firewall addrgrp
edit MGMT_IPs
```

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](#).

```
set service HTTPS HTTP
set schedule always
set status enable
next
edit 2
set intf any
set srcaddr all
set dstaddr all
set action deny
set service HTTPS HTTP
set schedule always
set status enable
end
```

If using non default ports, create appropriate service object for GUI administrative access:

```
config firewall service custom
edit GUI_HTTPS
set tcp-portrange admin-sport
next
edit GUI_HTTP
set tcp-portrange admin-port
end
```

Use these objects instead of 'HTTPS HTTP' in the local-in policy 1 and 2 below.

UPDATE: When using an HA reserved management interface, the local in policy needs to be configured slightly differently - please see:

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005>

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005>

Please contact customer support for assistance.

FortiProxy:

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 contact customer support for assistance.

FortiSwitchManager:

Disable HTTP/HTTPS administrative interface

Please contact customer support for assistance.

Version	Affected	Solution
FortiOS 7.2	7.2.0 through 7.2.1	Upgrade to 7.2.2 or above
FortiOS 7.0	7.0.0 through 7.0.6 (special below for FG6000F and 7000E models)	Upgrade to 7.0.7 or above
FortiOS 6.4	Not affected	Not Applicable
FortiOS 6.2	Not affected	Not Applicable
FortiProxy 7.2	7.2.0	Upgrade to 7.2.1 or above
FortiProxy 7.0	7.0.0 through 7.0.6	Upgrade to 7.0.7 or above
FortiProxy 2.0	Not affected	Not Applicable
FortiProxy 1.2	Not affected	Not Applicable
FortiProxy 1.1	Not affected	Not Applicable
FortiProxy 1.0	Not affected	Not Applicable
FortiSwitchManager	7.0.0	Upgrade to 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](#).



[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](#).