PSIRT

`Host` header injection

IR Number	**FG-IR-23-494**
Published Date	**Jan 14, 2025**
Updated Date	**Jan 7, 2026**
Component	**GUI**
Severity	**Medium**
CVSSv3 Score	**4.1**
Impact	**Improper access control**
CVE ID	**CVE-2022-23439**
Download	**CVRF**

Summary

FortiWLC 8.6 all versions
FortiWLC 8.5 all versions
FortiWLC 8.4 all versions
FortiVoice 7.2 all versions are not affected
FortiVoice version 7.0.0 through 7.0.1
FortiVoice version 6.4.0 through 6.4.8
FortiVoice version 6.0.0 through 6.0.11
FortiTester 7.4 all versions are not affected
FortiTester 7.3 all versions are not affected
FortiTester version 7.2.0 through 7.2.1
FortiTester 7.1 all versions
FortiTester 7.0 all versions
FortiTester 4.2 all versions
FortiTester 4.1 all versions
FortiTester 4.0 all versions
FortiTester 3.9 all versions
FortiTester 3.8 all versions
FortiTester 3.7 all versions
FortiTester 3.6 all versions
FortiTester 3.5 all versions
FortiTester 3.4 all versions
FortiTester 3.3 all versions
FortiSOAR on-premise 7.6 all versions are not affected
FortiSOAR on-premise 7.5 all versions are not affected
FortiSOAR on-premise 7.4 all versions are not affected
FortiSOAR on-premise 7.3 all versions are not affected
FortiSOAR on-premise 7.2 all versions
FortiSOAR on-premise 7.0 all versions
FortiSOAR on-premise 6.4 all versions
FortiRecorder 7.2 all versions are not affected
FortiRecorder 7.0 all versions are not affected

FortiProxy 1.2 all versions
FortiProxy 1.1 all versions
FortiProxy 1.0 all versions
FortiPortal 7.4 all versions are not affected
FortiPortal 7.2 all versions are not affected
FortiPortal 7.0 all versions are not affected
FortiPortal version 6.0.0 through 6.0.9
FortiOS 7.6 all versions are not affected
FortiOS 7.4 all versions are not affected
FortiOS version 7.2.0 through 7.2.4
FortiOS 7.0 all versions
FortiOS 6.4 all versions
FortiOS 6.2 all versions
FortiOS 6.0 all versions
FortiNDR 7.6 all versions are not affected
FortiNDR 7.4 all versions are not affected
FortiNDR version 7.2.0
FortiNDR version 7.1.0
FortiNDR 7.0 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
FortiManager 7.6 all versions are not affected
FortiManager version 7.4.0 through 7.4.3
FortiManager 7.2 all versions
FortiManager 7.0 all versions
FortiManager 6.4 all versions
FortiManager 6.2 all versions
FortiMail 7.6 all versions are not affected

FortiAuthenticator version 6.4.0 through 6.4.1
FortiAuthenticator version 6.3.0 through 6.3.3
FortiAuthenticator 6.2 all versions
FortiAuthenticator 6.1 all versions
FortiAuthenticator 6.0 all versions
FortiAuthenticator 5.5 all versions
FortiAuthenticator 5.4 all versions
FortiAuthenticator 5.3 all versions
FortiAuthenticator 5.2 all versions
FortiAuthenticator 5.1 all versions
FortiAnalyzer 7.6 all versions are not affected
FortiAnalyzer version 7.4.0 through 7.4.2
FortiAnalyzer 7.2 all versions
FortiAnalyzer 7.0 all versions
FortiAnalyzer 6.4 all versions
FortiAnalyzer 6.2 all versions
At least
FortiSwitch 7.6 all versions are not affected
FortiSwitch 7.4 all versions are not affected
FortiSwitch 7.2 all versions are not affected
FortiSwitch version 7.0.0 through 7.0.4
FortiSwitch version 6.4.0 through 6.4.10
FortiSwitch 6.2 all versions
FortiSwitch 6.0 all versions
At least
FortiDDoS-F 7.0 all versions are not affected
FortiDDoS-F 6.6 all versions are not affected
FortiDDoS-F 6.5 all versions are not affected
FortiDDoS-F 6.4 all versions are not affected
FortiDDoS-F version 6.3.0 through 6.3.3
FortiDDoS-F 6.2 all versions

FortiDDoS 5.0 all versions
FortiDDoS 4.7 all versions
FortiDDoS 4.6 all versions
FortiDDoS 4.5 all versions
At least
FortiADC 7.6 all versions are not affected
FortiADC 7.4 all versions are not affected
FortiADC 7.2 all versions are not affected
FortiADC 7.1 all versions are not affected
FortiADC version 7.0.0 through 7.0.1
FortiADC version 6.2.0 through 6.2.3
FortiADC 6.1 all versions
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

Solutions

FortiOS
Administrative Interface
Upgrade to FortiOS version 7.0.6 and above,
Upgrade to FortiOS version 7.2.1 and above.
AND
Set the `admin-host` property to the device hostname, which will disable `Host redirection`:

```
config system global
    set admin-host <string> "Administrative host for HTTP and HTTPs. When set, will be used in
```

Webfilter interface (port 8008)
Upgrade to FortiOS version 7.4.0 or above
Upgrade to FortiOS version 7.2.5 or above
Upgrade to FortiOS version 7.0.12 or above
Upgrade to FortiOS version 6.4.13 or above

FortiProxy
Administrative Interface
Upgrade to FortiProxy version 7.0.5 and above
AND
Set the `admin-host` property to the device hostname, which will disable `Host redirection`:
config system global
set admin-host <string> "Administrative host for HTTP and HTTPs. When set, will be used in lieu of the client's Host header for any redirection"

SSLVPN interface
Upgrade to FortiProxy version 7.4.0 or above
AND
Set the `server-hostname` property to the device hostname, which will disable `Host redirection` for SSL VPN:
config vpn ssl settings
set server-hostname Server hostname for HTTPS. When set, will be used for SSL VPN web proxy host header for any redirection.

WebFilter interface (port 8008)
Upgrade to FortiProxy version 7.4.0 or above

Upgrade to FortiRecorder version 7.0.0 or above
Upgrade to FortiRecorder version 6.4.3 or above
Upgrade to FortiRecorder version 6.0.11 or above
Upgrade to FortiNDR version 7.4.0 or above

FortiAnalyzer & FortiManager

Upgrade to version 7.6.0 or above

Set the `https-redirect-host` property to the device hostname, which will disable `Host redirection`:

```
config system global
    set https-redirect-host <string> "Administrative host for HTTP and HTTPs. When set, will be used in lieu of the client's Host header for any redirection"
end
```

FortiADC

Upgrade to FortiADC version 7.1.0 or above

Upgrade to FortiADC version 7.0.2 or above

Upgrade to FortiADC version 6.2.4 or above

AND

Set the `admin-host` property to the device hostname, which will disable `Host redirection`:

```
 config system global
    set admin-host <string> "Administrative host for HTTP and HTTPs. When set, will be used in lieu of the client's Host header for any redirection"
```

FortiDDOS-F

Upgrade to FortiDDoS-F version 6.4.0 or above

Upgrade to FortiDDoS-F version 6.3.4 or above

AND

Set the `admin-host` property to the device hostname, which will disable `Host redirection`:

```
 config system global
    set admin-host <string> "Administrative host for HTTP and HTTPs. When set, will be used in lieu of the client's Host header for any redirection"
```

Upgrade to FortiSwitch version 7.2.0 or above

Upgrade to FortiSwitch version 7.0.5 or above

Upgrade to FortiSwitch version 6.4.11 or above

Upgrade to FortiVoice version 7.0.2 or above

Upgrade to FortiVoice version 6.4.9 or above

Upgrade to FortiMail version 7.2.0 or above

Upgrade to FortiMail version 7.0.4 or above

Acknowledgement

Internally reported and discovered by Théo Leleu of Fortinet Product Security team.

Timeline

2025-01-14: Initial publication
2026-01-07: Adding FortiManager & FortiAnalyzer