



Path confusion vulnerability in GUI

IR Number **FG-IR-25-910**

Published Date **Nov 14, 2025**

Component **GUI**

Severity **⚠ Critical**

CVSSv3 Score **9.4**

Impact **Improper access control**

CVE ID **CVE-2025-64446**

Download **↓ CVRF**

↓ CSAF

Summary

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

Version	Affected	Solution
FortiWeb 8.0	8.0.0 through 8.0.1	Upgrade to 8.0.2 or above
FortiWeb 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
FortiWeb 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiWeb 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiWeb 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above

Workaround

Disable HTTP or HTTPS for internet facing interfaces. Fortinet recommends taking this action until an upgrade can be performed. If the HTTP/HTTPS Management interface is internally accessible only as per best practice, the risk is significantly reduced.

Post Upgrade Steps

It is recommended that customers review their configuration for and review logs for unexpected modifications, or the addition of unauthorized administrator accounts.

Timeline

2025-11-14: Initial publication

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](#).