



Unauthenticated remote command injection

IR Number **FG-IR-25-772**

Published Date **Jan 13, 2026**

Component **API**

Severity **⚠ Critical**

CVSSv3 Score **9.4**

Impact **Execute unauthorized code or commands**

CVE ID **CVE-2025-64155**

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
FortiSIEM 7.5	Not affected	Not Applicable
FortiSIEM 7.4	7.4.0	Upgrade to 7.4.1 or above
FortiSIEM 7.3	7.3.0 through 7.3.4	Upgrade to 7.3.5 or above
FortiSIEM 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiSIEM 7.1	7.1.0 through 7.1.8	Upgrade to 7.1.9 or above
FortiSIEM 7.0	7.0.0 through 7.0.4	Migrate to a fixed release
FortiSIEM 6.7	6.7.0 through 6.7.10	Migrate to a fixed release

This vulnerability does not impact Collector nodes, only the Super and Worker nodes.

Workaround

- Limit access to the phMonitor port (7900)

Acknowledgement

Fortinet is pleased to thank security researchers Zach Hanley (@hacks_zach) of Horizon3.ai for discovering and reporting this vulnerability under responsible disclosure.

Timeline

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](#).

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](#).