



CVE-2021-25268

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-25268 |
| State | PUBLIC |
| Assigner | security-alert@sophos.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-05-05 18:15:00 UTC |
| Updated | 2022-05-13 04:26:00 UTC |
| Description | Multiple XSS vulnerabilities in Webadmin allow for privilege escalation from MySophos admin to SFOS admin in Sophos Fi |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------------------|-----------------------------------|---------|--------|---------|----------|
| Hardware | Sophos | Firewall | - | All | All | All |
| Operating System | Sophos | Firewall Firmware | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|---------------------|
| www.sophos.com/en-us/security-advisories/sophos-sa-20220505-sfos-19-0-0 | CONFIRM | www.sophos.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

LEGACY: Gaetano Sapia

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)