



CVE-2018-19391

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-19391
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-15 16:29:00 UTC
Updated	2019-03-15 17:40:00 UTC
Description	Cobham Satcom Sailor 250 and 500 devices before 1.25 contained persistent XSS, which could be exploited by an unauth

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cobham	Satcom Sailor 250	-	All	All	All
Hardware	Cobham	Satcom Sailor 250	-	All	All	All
Operating System	Cobham	Satcom Sailor 250 Firmware	All	All	All	All
Operating System	Cobham	Satcom Sailor 250 Firmware	All	All	All	All
Hardware	Cobham	Satcom Sailor 500	-	All	All	All
Hardware	Cobham	Satcom Sailor 500	-	All	All	All
Operating System	Cobham	Satcom Sailor 500 Firmware	All	All	All	All
Operating System	Cobham	Satcom Sailor 500 Firmware	All	All	All	All

References

Reference

- CVE-2018-19391: The Cobham Satcom Sailor 250 and Sailor 500 devices contained a persistent Cross Site Scripting (XSS) vulnerability, whi
- CyberSKR - Cyber Security Consultancy
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)