



CVE-2018-19394

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

Summary

CVE	CVE-2018-19394
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 17:34:00 UTC
Description	Cobham Satcom Sailor 800 and 900 devices contained persistent XSS, which required administrative access to exploit. The

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 800	-	All	All	All
Hardware	Cobham	Satcom Sailor 800	-	All	All	All
Operating System	Cobham	Satcom Sailor 800 Firmware	-	All	All	All
Operating System	Cobham	Satcom Sailor 800 Firmware	-	All	All	All
Hardware	Cobham	Satcom Sailor 900	-	All	All	All
Hardware	Cobham	Satcom Sailor 900	-	All	All	All
Operating System	Cobham	Satcom Sailor 900 Firmware	-	All	All	All
Operating System	Cobham	Satcom Sailor 900 Firmware	-	All	All	All

References

Reference

[CyberSKR - Cyber Security Consultancy](#)

[CVE-2018-19394: The Cobham Satcom Sailor 800 and Sailor 900 devices contained a persistent Cross Site Scripting \(XSS\) vulnerability.](#) · GitHub

[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](#)