



CVE-2019-7418

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

Summary

CVE	CVE-2019-7418
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2019-03-25 14:20:00 UTC
Description	XSS exists in SAMSUNG X7400GX SyncThru Web Service V6.A6.25 V11.01.05.25_08-21-2015 in "/sws/swsAlert.sws" in r

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samsung	Syncthru Web Service	-	All	All	All
Application	Samsung	Syncthru Web Service	-	All	All	All
Hardware	Samsung	X7400gx	-	All	All	All
Hardware	Samsung	X7400gx	-	All	All	All
Operating System	Samsung	X7400gx Firmware	6.a6.25	All	All	All
Operating System	Samsung	X7400gx Firmware	6.a6.25	All	All	All

References

Reference

New URL

Full Disclosure: [CVE-2019-7418, CVE-2019-7419, CVE-2019-7420, CVE-2019-7421] Cross Site Scripting in SAMSUNG X7400GX Sync Thru

Home Electronics | Home Appliances | Mobile | Computing |

SAMSUNG X7400GX Sync Thru Web Cross Site Scripting ~ Packet Storm

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](#)