CVE-2017-6803

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-6803
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-20 16:59:00 UTC
Updated	2017-03-23 17:22:00 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the web interface in the Scheduler in SolarWinds (formerly Serv

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Solarwinds	Ftp Voyager	16.2.0	All	All	All
Application	Solarwinds	Ftp Voyager	16.2.0	All	All	All

References

Reference	Source	Link
FTP Voyager Scheduler CVE-2017-6803 Multiple Cross Site Request Forgery Vulnerabilities	BID	www.securityfocu
FTP Voyager Scheduler 16.2.0 - Cross-Site Request Forgery	EXPLOIT-DB	www.exploit-db.c
FTP Voyager Scheduler 16.2.0 CSRF / Denial Of Service ≈ Packet Storm	MISC	packetstormsecur
hyp3rlinx.altervista.org/advisories/FTP-VOYAGER-SCHEDULER-CSRF-REMOTE-CMD-EXECUTION.txt	MISC	hyp3rlinx.altervist
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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 registred 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