



CVE-2016-9500

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

Summary

CVE	CVE-2016-9500
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-13 20:29:00 UTC
Updated	2019-10-09 23:20:00 UTC
Description	Accellion FTP server prior to version FTA_9_12_220 uses the Accusoft Prizm Content flash component, which contains mu

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Accellion	Ftp Server	All	All	All	All
Application	Accellion	Ftp Server	All	All	All	All

References

Reference	Source	Link
www.qualys.com/2016/12/06/qlsa-2016-12-06/qlsa-2016-12-06.pdf	MISC	www
Accellion FTP server Information Disclosure and Cross-Site Scripting Vulnerabilities	BID	www
Vulnerability Note VU#745607 - Accellion FTP server contains information exposure and cross-site scripting vulnerabilities	CERT-VN	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks to Ashish Kamble for reporting this vulnerability.

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](#).

Free CVE JSON API [cve.report/api](#)

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