



CVE-2015-7676

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

Summary

CVE	CVE-2015-7676
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-15 15:59:00 UTC
Updated	2016-11-28 19:44:00 UTC
Description	Ipswitch MOVEit File Transfer (formerly DMZ) 8.1 and earlier, when configured to support file view on download, allows remote users to upload files to the server. This vulnerability could be exploited to upload a malicious file to the server, which could be used to execute arbitrary code on the server.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ipswitch	Moveit Dmz	All	All	All	All

References

Reference	Source	Link	Tags
Ipswitch MOVEit DMZ 8.1 Persistent Cross Site Scripting ~ Packet Storm	MISC	packetstormsecurity.com	Exploit
profundis-labs.com/advisories/CVE-2015-7676.txt	MISC	profundis-labs.com	Exploit
Full Disclosure: Multiple security issues in MOVEit Managed File Transfer application	FULLDISC	seclists.org	
Ipswitch MOVEit File Transfer CVE-2015-7676 HTML Injection Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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

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](#)