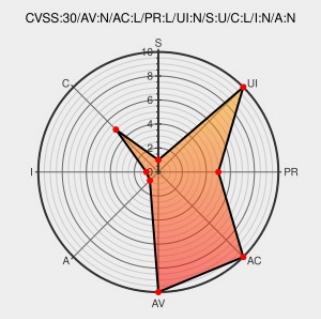
CVE-2018-18777

Published on: 11/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:53 PM UTC

CVE-2018-18777

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Microstrategy Web from Microstrategy contain the following vulnerability:

Directory traversal vulnerability in Microstrategy Web, version 7, in "/WebMstr7/servlet/mstrWeb" (in the parameter subpage) allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application. NOTE: this is a deprecated product.

CVE-2018-18777 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Microstrategy Web 7 - Cross-Site Scripting / Directory Traversal - JSP webapps Exploit	Exploit, Third Party Advisory	EXPLOIT-DB 45755

	VDB Entry www.exploit-db.com Proof of Concept text/html	
Microstrategy Web 7 Cross Site Scripting / Traversal ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/150059/Microstrategy-Web-7-Cross-Site-Scripting-Traversal.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microstrategy	Microstrategy Web	7	All	All	All
Application	Microstrategy	Microstrategy Web	7	All	All	All

cpe:2.3:a:microstrategy:microstrategy_web:7:*:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy_web:7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→