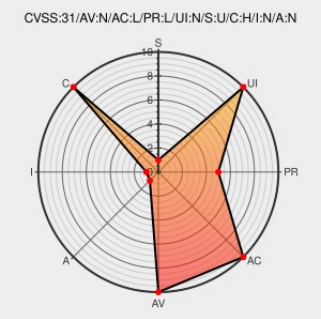
CVE-2020-24815

Published on: 11/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-24815

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



Certain versions of Microstrategy from Microstrategy contain the following vulnerability:

A Server-Side Request Forgery (SSRF) affecting the PDF generation in MicroStrategy 10.4, 2019 before Update 6, and 2020 before Update 2 allows authenticated users to access the content of internal network resources or leak files from the local system via HTML containers embedded in a dossier/dashboard document. NOTE: 10.4., no fix will be released as version will reach end-of-life on 31/12/2020.

CVE-2020-24815 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	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 Community	Vendor Advisory community.microstrategy.com	MISC community.microstrategy.com/s/article/Securing-PDF-and-Excel-Export-with-Whitelists?language=en_US

	text/html	
Extracting your AWS Access Keys through a PDF file - Triskele Labs	Exploit Third Party Advisory triskelelabs.com text/html	MISC triskelelabs.com/extracting-your-aws-access-keys-through-a-pdf-file/
Business Analytics & Mobility Solutions	Vendor Advisory microstrategy.com text/html	MISC microstrategy.com

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	10.4	All	All	All
Application	Microstrategy	Microstrategy	2019	update1	All	All
Application	Microstrategy	Microstrategy	2019	update2	All	All
Application	Microstrategy	Microstrategy	2019	update3	All	All
Application	Microstrategy	Microstrategy	2019	update4	All	All
Application	Microstrategy	Microstrategy	2019	update5	All	All
Application	Microstrategy	Microstrategy	2020	update1	All	All
Application	Microstrategy	Microstrategy	10.4	All	All	All
Application	Microstrategy	Microstrategy	2019	update1	All	All
Application	Microstrategy	Microstrategy	2019	update2	All	All
Application	Microstrategy	Microstrategy	2019	update3	All	All
Application	Microstrategy	Microstrategy	2019	update4	All	All
Application	Microstrategy	Microstrategy	2019	update5	All	All
Application	Microstrategy	Microstrategy	2020	update1	All	All

cpe:2.3:a:microstrategy:microstrategy:10.4:*:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update1:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update2:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update3:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update4:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update5:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2020:update1:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:10.4:*:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update1:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update2:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update3:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update4:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2019:update5:*:*:*:*:*:*:

cpe:2.3:a:microstrategy:microstrategy:2020:update1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→