

MicroStrategy Intelligence Server And Web 10.4 XSS / Disclosure / SSRF / Code Execution

Authored by redtimmysec | Site redtimmy.com

Posted Apr 2, 2020

MicroStrategy Intelligence Server and Web version 10.4 suffers from remote code execution, cross site scripting, server-side request forgery, and information disclosure vulnerabilities.

tags | exploit, remote, web, vulnerability, code execution, xss, info disclosure

advisories | CVE-2020-11450, CVE-2020-11451, CVE-2020-11452, CVE-2020-11453, CVE-2020-11454

SHA-256 | 2e452f25b0aabc3741eb00b4ee2e86d5d200045527146eae962c28cf79d36776 Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror Download

Exploit Title: MicroStrategy Intelligence Server and Web 10.4 - Multiple vulnerabilities
Exploit Author: RedTimmy Security
Authors blog: https://www.redtimmy.com/web-application-hacking/another-ssrf-another-rce-the-microstrategy-case/
Vendor Homepage: https://www.microstrategy.com/
Version(s): 10.4 and possibly above
CVE: CVE-2020-11450, CVE-2020-11451, CVE-2020-11452, CVE-2020-11453, CVE-2020-11454

Early last autumn we have conducted an assessment on MicroStrategy Intelligence Server & Web 10.4, that brought to the discovery of six different vulnerabilities and recently to the registration of a total of five CVE(s).

CVE-2020-11450 - Information Disclosure in Axis2 Happiness Page
Microstrategy Web 10.4 and possibly above exposes JVM configuration, CPU architecture, installation folder and other info through the URL "/MicroStrategyWS/happyaxis.jsp". An attacker could use this vulnerability to learn more about the environment the application is running in.

CVE-2020-11453 - Server-Side Request Forgery in Test Web Service
Microstrategy Web 10.4 and possibly above is vulnerable to Server-Side Request Forgery in the "Test Web Service" functionality exposed through the path "/MicroStrategyWS/". The functionality requires no authentication and, while it is not possible to pass arbitrary schemes and parameters in the SSRF request, it is still possible to exploit it to conduct port scanning. An attacker could exploit this vulnerability to enumerate the resources allocated in the network (IP addresses and services exposed).

CVE-2020-11452- Server Side Request Forgery in adding external data
Microstrategy Web 10.4 and possibly above includes a functionality to allow users to import files or data from external resources such as URLs or databases in order to parse contents for dashboard creation. By providing an external URL under attacker control it's possible to send requests to external resources or leak files from the local system using the "file://" stream wrapper.

CVE-2020-11451 - Remote Code Execution in Upload Visualization Plugin
The "Upload Visualization" plugin in the Microstrategy admin panel (version 10.4 and above) allows an administrator to upload a zip archive containing files with arbitrary extensions and data. Access to admin panel could be reached through SSRF (for example via CVE-2020-11452).

CVE-2020-11454 - Stored Cross-Site Scripting in the Dashboard
Microstrategy Web 10.4 and possibly above is vulnerable to Stored Cross-Site Scripting in the "HTML Containers" and "Insert Text" functionalities in the window allowing for the creation of a new dashboard. In order to exploit this vulnerability an user need to have access to a shared dashboard or the ability to create a dashboard on the application.

More details and full story here:
https://www.redtimmy.com/web-application-hacking/another-ssrf-another-rce-the-microstrategy-case/

Login or Register to add favorites

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

December 2022

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

Older

Systems

AIX (426)

Apple (1,926)

BSD (370)

CentOS (55)

Cisco (1,917)

Debian (6,634)

Fedora (1,690)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

IOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,315)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,469)

Slackware (941)

Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed