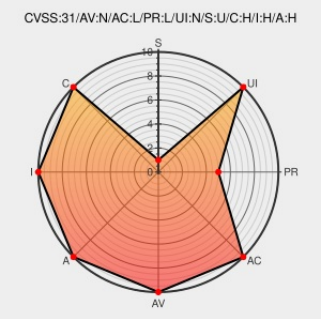
CVE-2021-36359

Published on: 08/30/2021 12:00:00 AM UTC

Last Modified on: 09/01/2021 08:14:00 PM UTC

CVE-2021-36359

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



Certain versions of Bscw Classic from Bscw contain the following vulnerability:

OrbiTeam BSCW Classic before 7.4.3 allows exportpdf authenticated remote code execution (RCE) via XML tag injection because reportlab\platypus\paraparser.py (reached via bscw.cgi op=_editfolder.EditFolder) calls eval on attacker-supplied Python code. This is fixed in 5.0.12, 5.1.10, 5.2.4, 7.3.3, and 7.4.3.

CVE-2021-36359 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
BSCW Server XML Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163988/BSCW-Server-XML-Injection.html

Full Disclosure: SEC Consult SA-20210827-1 :: XML Tag injection in BSCW Server	seclists.org text/html	FULLDISC 20210827 SEC Consult SA-20210827-1 :: XML Tag injection in BSCW Server
Company – BSCW | Groupware for efficient teamwork and document management	www.bscw.de text/html	MISC www.bscw.de/en/company/

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2021-36359 : OrbiTeam BSCW Classic before 7.4.3 allows exportpdf authenticated remote code exe…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bscw	Bscw Classic	All	All	All	All

cpe:2.3:a:bscw:bscw_classic:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-36359 : OrbiTeam BSCW Classic before 7.4.3 allows exportpdf authenticated remote code execution RCE via… twitter.com/i/web/status/1…	2021-08-30 05:09:06
@SecRiskRptSME	RT: CVE-2021-36359 OrbiTeam BSCW Classic before 7.4.3 allows exportpdf authenticated remote code execution (RCE) v… twitter.com/i/web/status/1…	2021-08-30 07:33:47
@LinInfoSec	Python - CVE-2021-36359: bscw.de/en/company/	2021-08-30 16:29:34

← Previous ID

Next ID→