



CVE-2022-27665

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2022-27665
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-03 14:15:00 UTC
Updated	2024-02-01 01:04:00 UTC
Description	Reflected XSS (via AngularJS sandbox escape expressions) exists in Progress Ipswitch WS_FTP Server 8.6.0. This can le

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Progress	Ipswitch Ws Ftp Server	8.6.0	All	All	All
Application	Progress	Ws Ftp Server	8.6.0	All	All	All

References

Reference	Source
GitHub - dievus/CVE-2022-27665: Reflected XSS via AngularJS Sandbox Escape Expressions in IPSwitch WS_FTP Server 8.6.0	MISC
What's New in WS_FTP Server 2020	MISC
Progress Customer Community	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[27395](#) Progress WS_FTP Server Multiple Vulnerabilities

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)