



CVE-2023-2989

Published on: Not Yet Published

Last Modified on: 06/30/2023 07:21:00 PM UTC

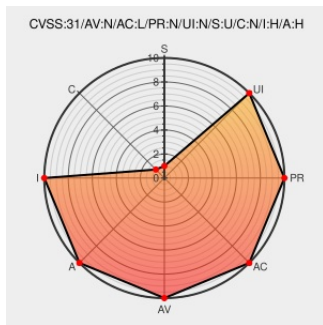
CVE-2023-2989

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Eft Server](#) from [Globalscape](#) contain the following vulnerability:

Fortra Globalscape EFT versions before 8.1.0.16 suffer from an out of bounds memory read in their administration server, which can allow an attacker to crash the service or bypass authentication if successfully exploited

CVE-2023-2989 has been assigned by cve@rapid7.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Fortra - Globalscape EFT** version < **8.1.0.16**

CVSS3 Score: **9.1 - CRITICAL**

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

CVE References

Description	Tags	Link
Multiple Vulnerabilities in Fortra Globalscape EFT Administration Server [FIXED] Rapid7 Blog	www.rapid7.com text/html	MISC www.rapid7.com/blog/post/2023/06/22/multiple-vulnerabilities-in-fortra-globalscape-eft-administration-server-fixed/
Is EFT susceptible to the "Authentication Bypass via Out-of-bounds Memory Read " vulnerability?	kb.globalscape.com text/html	MISC kb.globalscape.com/Knowledgebase/11586/Is-EFT-susceptible-to-the-Authentication-Bypass-via-Outofbounds-Memory-Read-vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Globalscape	Eft Server	All	All	All	All
cpe:2.3:a:globalscape:eft_server:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @noperator	CVE-2023-2989 (auth bypass via out-of-bounds read) is a really creative attack. Nice work @iagox86! Enjoyed reading. twitter.com/iagox86/status/1...	2023-06-22 18:53:26
 @CVereport	CVE-2023-2989 : Fortra Globalscape EFT versions before 8.1.0.16 suffer from an out of bounds memory read in their a... twitter.com/i/web/status/1...	2023-06-22 20:06:16
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-2989 Fortra Globalscape EFT versions before 8.1.0.16 suffer from an out... twitter.com/i/web/status/1...	2023-06-22 21:11:02
 @autumn_good_35	ファイル転送製品で理論上RCEの可能性もある脆弱性FIX。現時点では悪用出来る可能性は極めて低いとのことですが、計画的な対応を推奨との事 CVE-2023-2989、CVE-2023-2990、CVE-2023-2991 Mul... twitter.com/i/web/status/1...	2023-06-26 09:44:21

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report