



CVE-2021-29281

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-29281
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-07 21:15:00 UTC
Updated	2022-07-15 02:08:00 UTC
Description	File upload vulnerability in GFI Mail Archiver versions up to and including 15.1 via insecure implementation of Telerik Web U

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gfi	Archiver	All	All	All	All

References

Reference	Source	Link
Email Archiving Solutions for Exchange, Office 365 and other servers GFI Archiver	MISC	www.gfi.com
CWE - CWE-434: Unrestricted Upload of File with Dangerous Type (4.3)	MISC	cwe.mitre.org
GFI Mail Archiver 15.1 - Telerik UI Component Arbitrary File Upload (Unauthenticated) Exploit - Amin Bohio	MISC	aminbohio.com
Unrestricted File Upload OWASP Foundation	MISC	owasp.org
GFI Mail Archiver 15.1 - Telerik UI Component Arbitrary File Upload (Unauthenticated) - Multiple webapps Exploit	MISC	www.exploit-db.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

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