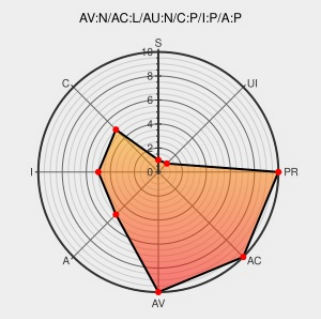
CVE-2005-4174

Published on: 12/11/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4174

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



Certain versions of Efiction from Efiction Project contain the following vulnerability:

eFiction 1.0, 1.1, and 2.0, in unspecified environments, might allow remote attackers to conduct unauthorized operations by directly accessing (1) install.php or (2) upgrade.php. NOTE: it is unclear whether this is a vulnerability in eFiction itself or the result of incorrect system administration practices, e.g. by not removing utility scripts once they have been used.

CVE-2005-4174 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
eFiction :: View topic - Full Disclosure for eFiction	www.efiction.wallflowergirl.com text/html	CONFIRM www.efiction.wallflowergirl.com/forums/viewtopic.php?t=1555
CXSecurity - IDS	securityreason.com text/html	SREASON 206
SecurityTracker.com Archives - eFiction Input Validation Holes Let Remote Users Inject SQL Commands, Conduct Cross-Site Scripting Attacks, and Execute Arbitrary Code	Exploit securitytracker.com text/html	SECTRACK 1015273
	Exploit Vendor Advisory	MISC rgod.altervista.org/efiction2_xpl.html

	rgod.altervista.org application/octet-stream Inactive Link Not Archived	
eFiction Multiple Input Validation Vulnerabilities	Exploit cve.report (archive) text/html	BID 15568
No Description Provided	Exploit Vendor Advisory archives.neohapsis.com Inactive Link Not Archived	BUGTRAQ 20051125 eFiction <= 2.0 multiple vulnerabilities
Secunia - Advisories - eFiction Multiple Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 17777

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	Efiction Project	Efiction	1.0	All	All	All
Application	Efiction Project	Efiction	1.1	All	All	All
Application	Efiction Project	Efiction	2.0	All	All	All
Application	Efiction Project	Efiction	1.0	All	All	All
Application	Efiction Project	Efiction	1.1	All	All	All
Application	Efiction Project	Efiction	2.0	All	All	All

cpe:2.3:a:efiction_project:efiction:1.0:*:*:*:*:*:*:*

cpe:2.3:a:efiction_project:efiction:1.1:*:*:*:*:*:*:*

cpe:2.3:a:efiction_project:efiction:2.0:*:*:*:*:*:*:*

cpe:2.3:a:efiction_project:efiction:1.0:*:*:*:*:*:*:*

cpe:2.3:a:efiction_project:efiction:1.1:*:*:*:*:*:*:*

cpe:2.3:a:efiction_project:efiction:2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← 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 registred 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