



CVE-2005-4171

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

Last Modified on: 03/23/2021 11:27:22 PM UTC

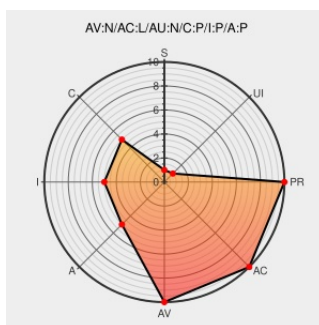
CVE-2005-4171

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Efiction](#) from [Efiction Project](#) contain the following vulnerability:

The "Upload new image" command in the "Manage Images" eFiction 1.1, when members are allowed to upload images, allows remote attackers to execute arbitrary PHP code by uploading a filename with a .php extension that contains a GIF header, which passes the image validity check but executes any PHP code within the file.

CVE-2005-4171 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

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

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
rgod.altervista.org
application/octet-stream
Inactive Link **Not Archived**

MISC rgod.altervista.org/efiction2_xpl.html

No Description Provided

[www.osvdb.org](#)

OSVDB 21124

Inactive LinkNot Archived

eFiction Multiple Input Validation Vulnerabilities

Exploit
cve.report (archive)
text/html

BID 15568

No Description Provided

Exploit
Vendor Advisory
archives.neohapsis.com

BUGTRAQ 20051125 eFiction <= 2.0 multiple vulnerabilities

Inactive LinkNot Archived

Secunia - Advisories - eFiction Multiple Vulnerabilities

Exploit
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	1.1	All	All	All
Application	Efiction Project	Efiction	1.1	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →