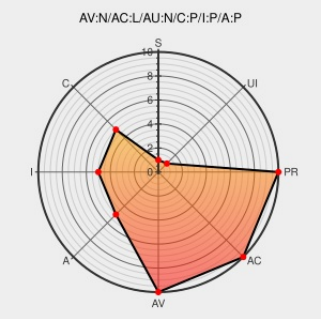
CVE-2004-2065

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2065

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



Certain versions of Dansguardian from Daniel Barron contain the following vulnerability:

DansGuardian 2.8 and earlier allows remote attackers to bypass the extension filtering rule via a hex encoded extension or . in the filename.

CVE-2004-2065 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
DansGuardian Hex Encoded File Extension URI Content Filter Bypass Vulnerability	Patch, cve.report (archive), text/html	BID 10823
No Description Provided	marc.info, text/html	BUGTRAQ 20040729 DansGuardian Hex Encoding URL Banned Extension Filter Bypass
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 8270
No Description Provided	dansguardian.org, text/html	CONFIRM dansguardian.org/?page=history
DansGuarding File Extension Filter Can Be Bypassed With Hex-Encoded URLs - SecurityTracker	securitytracker.com, text/html	SECTRACK 1010817

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF dansguardian-filename-bypass-filtering(16836)
Secunia - Advisories - DansGuardian Banned Extension Filter Bypass Vulnerability	Patch web.archive.org text/html	SECUNIA 12191

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	Daniel Barron	Dansguardian	2.2.10	All	All	All
Application	Daniel Barron	Dansguardian	2.2.4	All	All	All
Application	Daniel Barron	Dansguardian	2.2.5	All	All	All
Application	Daniel Barron	Dansguardian	2.2.6	All	All	All
Application	Daniel Barron	Dansguardian	2.2.7	All	All	All
Application	Daniel Barron	Dansguardian	2.2.7.1	All	All	All
Application	Daniel Barron	Dansguardian	2.2.8	All	All	All
Application	Daniel Barron	Dansguardian	2.2.9	All	All	All
Application	Daniel Barron	Dansguardian	2.2.9.1	All	All	All
Application	Daniel Barron	Dansguardian	2.4.5.1	All	All	All
Application	Daniel Barron	Dansguardian	2.6.1.5	All	All	All
Application	Daniel Barron	Dansguardian	2.7.3.1	All	All	All
Application	Daniel Barron	Dansguardian	2.8	All	All	All
Application	Daniel Barron	Dansguardian	2.2.10	All	All	All
Application	Daniel Barron	Dansguardian	2.2.4	All	All	All
Application	Daniel Barron	Dansguardian	2.2.5	All	All	All
Application	Daniel Barron	Dansguardian	2.2.6	All	All	All
Application	Daniel Barron	Dansguardian	2.2.7	All	All	All
Application	Daniel Barron	Dansguardian	2.2.7.1	All	All	All
Application	Daniel Barron	Dansguardian	2.2.8	All	All	All
Application	Daniel Barron	Dansguardian	2.2.9	All	All	All
Application	Daniel Barron	Dansguardian	2.2.9.1	All	All	All
Application	Daniel Barron	Dansguardian	2.4.5.1	All	All	All
Application	Daniel Barron	Dansguardian	2.6.1.5	All	All	All

Application	Daniel Barron	Dansguardian	2.7.3.1	All	All	All
Application	Daniel Barron	Dansguardian	2.8	All	All	All

- cpe:2.3:a:daniel_barron:dansguardian:2.2.10:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.4:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.5:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.6:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.7:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.7.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.8:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.9:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.9.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.4.5.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.6.1.5:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.7.3.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.8:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.10:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.4:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.5:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.6:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.7:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.7.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.8:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.9:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.2.9.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.4.5.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.6.1.5:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.7.3.1:*:*:*:*:*:*:*:
- cpe:2.3:a:daniel_barron:dansguardian:2.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→