

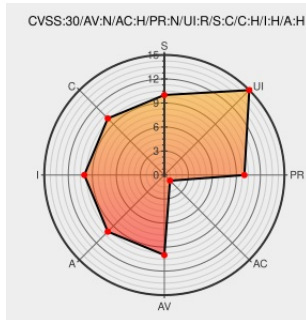


CVE-2017-2792

Published on: 09/07/2018 12:00:00 AM UTC

Last Modified on: 04/19/2022 07:15:00 PM UTC

CVE-2017-2792

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

An exploitable heap corruption vulnerability exists in the iBldDirInfo functionality of Antenna House DMC HTMLFilter used by MarkLogic 8.0-6. A specially crafted xls file can cause a heap corruption resulting in arbitrary code execution. An attacker can provide a malicious xls file to trigger this vulnerability.

CVE-2017-2792 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Antenna House](#) - **DMC HTMLFilter** version **as shipped with MarkLogic 8.0-6**

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
TALOS-2017-0284 Cisco Talos Intelligence Group -	Third Party Advisory	MISC

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	Marklogic	Marklogic	8.0-6	All	All	All
Application	Marklogic	Marklogic	8.0-6	All	All	All
cpe:2.3:a:marklogic:marklogic:8.0-6:~::~~::~~::~~::~~::~~::~::						
cpe:2.3:a:marklogic:marklogic:8.0-6:~::~~::~~::~~::~~::~~::~::						

No vendor comments have been submitted for this CVE