CVE-2017-2798

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-2798
State	PUBLISHED
Assigner	talos
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-24 14:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	An exploitable heap corruption vulnerability exists in the GetIndexArray functionality of Antenna House DMC HTMLFilter as

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Problem Types: CWE-119 | heap overflow

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.0	talos-cna@cisco.com	Secondary	8.3	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
3.0	CNA	DECLARED	8.3	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Marklogic	Marklogic	8.0-6	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Antenna House	DMC HTMLFilter	affected as shipped with Marklogic 8.0-6	Not specified

References

Reference	Source	Link
TALOS-2017-0291 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	af854a3a-2127-422b-91ae-364da2661108	talos
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report