



CVE-2020-12460

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-12460
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-27 23:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0-Beta1 has improper null termination in the function opendmarc_xml_pa

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Trusteddomain	Opendmarc	1.4.0	beta0	All	All
Application	Trusteddomain	Opendmarc	1.4.0	beta1	All	All
Application	Trusteddomain	Opendmarc	1.4.0	beta0	All	All
Application	Trusteddomain	Opendmarc	1.4.0	beta1	All	All
Application	Trusteddomain	Opendmarc	All	All	All	All

References

Reference	Source	Link	T
[SECURITY] Fedora 34 Update: opendmarc-1.4.0-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Memory corruption in opendmarc_xml() · Issue #64 · trusteddomainproject/OpenDMARC · GitHub	MISC	github.com	E
[SECURITY] Fedora 34 Update: opendmarc-1.4.1-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: opendmarc-1.4.1-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: opendmarc-1.4.1-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: opendmarc-1.4.1-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

opendmarc Free Communications software downloads at SourceForge.net	MISC	sourceforge.net	F
[SECURITY] Fedora 34 Update: opendmarc-1.4.0-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2639-1] opendmarc security update	MLIST	lists.debian.org	
OpenDMARC: Heap-based buffer overflow (GLSA 202011-02) — Gentoo security	GENTOO	security.gentoo.org	T
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178648](#) Debian Security Update for opendmarc (DLA 2639-1)
- [281112](#) Fedora Security Update for opendmarc (FEDORA-2021-1ec3c5ed63)
- [281113](#) Fedora Security Update for opendmarc (FEDORA-2021-433e7d72ce)
- [281233](#) Fedora Security Update for opendmarc (FEDORA-2021-c1b846164e)
- [690760](#) Free Berkeley Software Distribution (FreeBSD) Security Update for opendmarc - Multiple Vulnerabilities (937aa1d6-685e-11ec-a636-000c29061ce6)

© [CVE.report](#) 2026 |

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 registered 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](#).

Free CVE JSON API cve.report/api

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