



CVE-2022-26662

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

Summary

CVE	CVE-2022-26662
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-10 17:47:00 UTC
Updated	2022-03-18 15:07:00 UTC
Description	An XML Entity Expansion (XEE) issue was discovered in Tryton Application Platform (Server) 5.x through 5.0.45, 6.x through 6.0.45, and 7.x through 7.0.45. The issue is caused by a lack of input validation in the XML parser, which allows an attacker to craft a malicious XML document that can cause a denial of service (DoS) attack. The issue is fixed in Tryton Application Platform (Server) 5.0.46, 6.0.46, and 7.0.46.

Risk And Classification

Problem Types: CWE-776

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Tryton	Proteus	All	All	All	All
Application	Tryton	Trytond	All	All	All	All

References

Reference
[SECURITY] [DLA 2946-1] tryton-proteus security update
[SECURITY] [DLA 2945-1] tryton-server security update
Debian -- Security Information -- DSA-5098-1 tryton-server
Security Release for issue11219 and issue11244 - News - Tryton Discussion
Issue 11244: A non authenticated user can cause a denial of service with a single request using an xml bomb attack on xmlrpc - Tryton issue 11244
Debian -- Security Information -- DSA-5099-1 tryton-proteus
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179124 Debian Security Update for tryton-server (DLA 2945-1)
179125 Debian Security Update for tryton-proteus (DLA 2946-1)
179141 Debian Security Update for tryton-server (DSA 5098-1)
179147 Debian Security Update for tryton-proteus (DSA 5099-1)
183136 Debian Security Update for tryton-servertryton-proteus (CVE-2022-26662)

© [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](#)