



CVE-2020-7351

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

Summary

CVE	CVE-2020-7351
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-01 16:15:00 UTC
Updated	2022-04-18 09:37:00 UTC
Description	An OS Command Injection vulnerability in the endpoint_devicemap.php component of Fonality Trixbox Community Edition :

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netfortis	Trixbox	All	All	All	All
Application	Netfortis	Trixbox	All	All	All	All

References

Reference

- [Trixbox CE v2.8.0.4 endpoint_devicemap.php Authenticated Remote Command Execution by stasinopoulos · Pull Request #13353 · rapid7/m...](#)
- [TrixBox CE 2.8.0.4 Command Execution ≈ Packet Storm](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered and reported by Anastasios Stasinopoulos.

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

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)