



CVE-2020-6655

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

Summary

CVE	CVE-2020-6655
State	PUBLIC
Assigner	CybersecurityCOE@eaton.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-07 18:15:00 UTC
Updated	2021-03-31 12:48:00 UTC
Description	The Eaton's easySoft software v7.xx prior to v7.22 are susceptible to Out-of-bounds remote code execution vulnerability. A

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eaton	Easysoft	All	All	All	All
Application	Eaton	Easysoft	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-20-1443 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Ac
www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/securit...	MISC	www.eaton.com	Vendor Advise
Eaton EASYsoft CISA	MISC	us-cert.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

LEGACY: Eaton would like to thank Francis Provencher from ZDI

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](#)