



CVE-2018-12596

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

Summary

CVE	CVE-2018-12596
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-10 21:29:00 UTC
Updated	2023-11-07 02:52:00 UTC
Description	Episerver Ektron CMS before 9.0 SP3 Site CU 31, 9.1 before SP3 Site CU 45, or 9.2 before SP2 Site CU 22 allows remote

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Episerver	Ektron Cms	9.00	-	All	All
Application	Episerver	Ektron Cms	9.00	sp1	All	All
Application	Episerver	Ektron Cms	9.00	sp2	All	All
Application	Episerver	Ektron Cms	9.10	-	All	All
Application	Episerver	Ektron Cms	9.10	sp1	All	All
Application	Episerver	Ektron Cms	9.10	sp2	All	All
Application	Episerver	Ektron Cms	9.20	-	All	All
Application	Episerver	Ektron Cms	9.20	sp1	All	All
Application	Episerver	Ektron Cms	9.00	-	All	All
Application	Episerver	Ektron Cms	9.00	sp1	All	All
Application	Episerver	Ektron Cms	9.00	sp2	All	All
Application	Episerver	Ektron Cms	9.10	-	All	All
Application	Episerver	Ektron Cms	9.10	sp1	All	All
Application	Episerver	Ektron Cms	9.10	sp2	All	All
Application	Episerver	Ektron Cms	9.20	-	All	All
Application	Episerver	Ektron Cms	9.20	sp1	All	All

References

Reference	Source
GitHub - alt3kx/CVE-2018-12596: Ektron Content Management System (CMS) 9.20 SP2, remote re-enabling users (CVE-2018-12596)	MIS
Ektron CMS 9.20 SP2 - Improper Access Restrictions - ASPX webapps Exploit	EXP
Full Disclosure: Ektron Content Management System (CMS) 9.20 SP2, remote re-enabling users (CVE-2018-12596)	FULL
Ektron Content Management System (CMS) 9.20 SP2, remote re-enabling users (CVE-2018-12596) by alt3kx Medium	
Ektron Content Management System (CMS) 9.20 SP2, remote re-enabling users (CVE-2018-12596) by alt3kx Medium	MIS
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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](#).

Free CVE JSON API [cve.report/api](#)

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