



CVE-2017-6777

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

Summary

CVE	CVE-2017-6777
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-17 20:29:00 UTC
Updated	2017-08-22 17:59:00 UTC
Description	A vulnerability in the ConfD server of the Cisco Elastic Services Controller (ESC) could allow an authenticated, remote attac

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Elastic Services Controller	2.3	All	All	All
Application	Cisco	Elastic Services Controller	2.3(2)	All	All	All
Application	Cisco	Elastic Services Controller	2.3\2\	All	All	All
Application	Cisco	Elastic Services Controller	2.3	All	All	All
Application	Cisco	Elastic Services Controller	2.3\2\	All	All	All

References

Reference	Source	Link	Tags
Cisco Elastic Services Controller Configuration Parameters Information Disclosure Vulnerability	CISCO	tools.cisco.com	Venc
Cisco Elastic Services Controller CVE-2017-6777 Information Disclosure Vulnerability	BID	www.securityfocus.com	Thir
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

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](#)