



CVE-2018-0106

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

Summary

CVE	CVE-2018-0106
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-18 06:29:00 UTC
Updated	2020-09-04 17:12:00 UTC
Description	A vulnerability in the ConfD server of the Cisco Elastic Services Controller (ESC) could allow an unauthenticated, local attacker to execute arbitrary code on the target device. The vulnerability is due to a buffer overflow in the ConfD server. An attacker could exploit this vulnerability to execute arbitrary code on the target device. The vulnerability is present in Cisco Elastic Services Controller versions 5.0.0 through 5.0.1. Cisco has released a software update to address this vulnerability. Users are advised to upgrade to the latest version of the software.

Risk And Classification

Problem Types: CWE-552

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Elastic Services Controller	All	All	All	All
Application	Cisco	Elastic Services Controller	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Elastic Services Controller CVE-2018-0106 Local Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party
Cisco Elastic Services Controller Information Disclosure Vulnerability	CONFIRM	tools.cisco.com	Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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