



CVE-2016-9485

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

Summary

CVE	CVE-2016-9485
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-13 20:29:00 UTC
Updated	2019-10-09 23:20:00 UTC
Description	On Windows endpoints, the SecureConnector agent must run under the local SYSTEM account or another administrator ac

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Forescout	Secureconnector	-	All	All	All
Application	Forescout	Secureconnector	-	All	All	All

References

Reference	Source	Link
Vulnerability Note VU#768331 - ForeScout CounterACT SecureConnector agent is vulnerable to privilege escalation	CERT-VN	www.kb.c
ForeScout CounterACT SecureConnector Agent Multiple Insecure File Creation Vulnerabilities	BID	www.secd
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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