



CVE-2017-3141

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

Summary

CVE	CVE-2017-3141
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-16 20:29:00 UTC
Updated	2019-10-09 23:27:00 UTC
Description	The BIND installer on Windows uses an unquoted service path which can enable a local user to achieve privilege escalation

Risk And Classification

Problem Types: CWE-428

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Bind	9.2.6	p2	All	All
Application	isc	Bind	9.3.2	p1	All	All
Application	isc	Bind	9.2.6	p2	All	All
Application	isc	Bind	9.3.2	p1	All	All
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All
Application	isc	Bind	All	All	All	All

References

Reference	Source	Link
CVE-2017-3141: Windows service and uninstall paths are not quoted when BIND is installed - Security Advisories	CONFIRM	kb.isc.org
BIND Windows Installer Unquoted Service Path Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.secu
BIND 9.10.5 - Unquoted Service Path Privilege Escalation	EXPLOIT-DB	www.expl
June 2017 ISC BIND Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.n

ISC BIND CVE-2017-3141 Local Privilege Escalation Vulnerability	BID	www.secd
BIND: Multiple vulnerabilities (GLSA 201708-01) — Gentoo Security	GENTOO	security.g
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank John Page aka hyp3rlinx for reporting this issue.

Legacy QID Mappings

[710473](#) Gentoo Linux BIND Multiple Vulnerabilities (GLSA 201708-01)

© 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