



CVE-2019-3999

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

Summary

CVE	CVE-2019-3999
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-25 19:15:00 UTC
Updated	2022-01-01 19:30:00 UTC
Description	Improper neutralization of special elements used in an OS command in Druva inSync Windows Client 6.5.0 allows a local, u

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Druva	Insync Client	6.5.0	All	All	All
Application	Druva	Insync Client	6.5.0	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

References

Reference	Source	Link	Tags
Druva inSync Windows Client 6.5.2 Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
Druva inSync inSyncCPHwnet64.exe RPC Type 5 Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
Druva inSync Client Multiple Vulnerabilities - Research Advisory Tenable®	MISC	www.tenable.com	Exploit, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

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](#)