



CVE-2018-19636

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

Summary

CVE	CVE-2018-19636
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-05 16:29:00 UTC
Updated	2023-11-07 02:55:00 UTC
Description	Supportutils, before version 3.1-5.7.1, when run with command line argument -A searched the file system for a ndspath bin:

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensuse	Supportutils	All	All	All	All
Application	Opensuse	Supportutils	All	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2019:1351-1: important: Security update		lists.opensuse.org
Bug 1117751 – VUL-0: CVE-2018-19636: supportutils: Local root exploit via inclusion of attacker controlled shell script	CONFIRM	bugzilla.suse.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Vítězslav Čížek of SUSE

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)