



CVE-2017-1000082

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

Summary

CVE	CVE-2017-1000082
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-07 17:29:00 UTC
Updated	2022-01-31 18:22:00 UTC
Description	systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. "0day"), running the service in q

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freedesktop	Systemd	All	All	All	All
Application	Systemd Project	Systemd	All	All	All	All

References

Reference
systemd can't handle the process privilege that belongs to user name startswith number, such as 0day · Issue #6237 · systemd/systemd · Git
oss-security - systemd fails to parse user that should run service
systemd CVE-2017-1000082 Local Privilege Escalation Vulnerability
systemd Username Validation Flaw Lets Local Users Start Services With Higher Privileges Than Expected - SecurityTracker
CVE Program record
NVD vulnerability detail

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](#)