



CVE-2021-3551

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

Summary

CVE	CVE-2021-3551
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-16 17:15:00 UTC
Updated	2022-02-28 15:51:00 UTC
Description	A flaw was found in the PKI-server, where the spkispawn command, when run in debug mode, stores admin credentials in t

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dogtagpki	Dogtagpki	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Oracle	Linux	8	-	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.4	All	All	All

References

Reference	S
1959971 – (CVE-2021-3551) CVE-2021-3551 pki-server: Doataa installer "pkispawn" loas admin credentials into a world-readable log file	N

CVE Program record

C

NVD vulnerability detail

N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159243](#) Oracle Enterprise Linux Security Update for pki-core:10.6 (ELSA-2021-2235)

[239366](#) Red Hat Update for pki-core:10.6 (RHSA-2021:2235)

[281641](#) Fedora Security Update for dogtag (FEDORA-2021-99ca984f32)

[281642](#) Fedora Security Update for dogtag (FEDORA-2021-54a73a7112)

[377114](#) Alibaba Cloud Linux Security Update for pki-core:10.6 (ALINUX3-SA-2021:0037)

[940420](#) AlmaLinux Security Update for pki-core:10.6 (ALSA-2021:2235)

[960030](#) Rocky Linux Security Update for pki-core:10.6 (RLSA-2021:2235)

© [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](#)