



CVE-2021-20179

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

Summary

CVE	CVE-2021-20179
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-15 13:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A flaw was found in pki-core. An attacker who has successfully compromised a key could use this flaw to renew the correspo

Risk And Classification

Problem Types: CWE-863

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	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Redhat	Certificate System	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Li
CVE-2021-20179: Fix renewal profile approval process - v10.5 by cipherboy · Pull Request #3478 · dogtagpki/pki · GitHub	MISC	git
[SECURITY] Fedora 33 Update: pki-core-10.10.5-5.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	list
CVE-2021-20179: Fix renewal profile approval process - v10.11 by cipherboy · Pull Request #3474 · dogtagpki/pki · GitHub	MISC	git
[SECURITY] Fedora 32 Update: pki-core-10.10.5-5.fc32 - package-announce - Fedora Mailing-Lists		list
CVE-2021-20179: Fix renewal profile approval process - v10.10 by cipherboy · Pull Request #3475 · dogtagpki/pki · GitHub	MISC	git
CVE-2021-20179: Fix renewal profile approval process - v10.9 by cipherboy · Pull Request #3476 · dogtagpki/pki · GitHub	MISC	git
[SECURITY] Fedora 32 Update: pki-core-10.10.5-5.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	list

CVE-2021-20179: Fix renewal profile approval process - v10.8 by cipherboy · Pull Request #3477 · dogtagpki/pki · GitHub	MISC	git
[SECURITY] Fedora 34 Update: dogtag-pki-10.10.5-3.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	list
[SECURITY] Fedora 33 Update: pki-core-10.10.5-5.fc33 - package-announce - Fedora Mailing-Lists		list
1914379 – (CVE-2021-20179) CVE-2021-20179 pki-core: Unprivileged users can renew any certificate	MISC	bu
[SECURITY] Fedora 34 Update: dogtag-pki-10.10.5-3.fc34 - package-announce - Fedora Mailing-Lists		list
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159122](#) Oracle Enterprise Linux Security Update for pki-core:10.6 (ELSA-2021-0966)

[179649](#) Debian Security Update for dogtag-pki (CVE-2021-20179)

[239176](#) Red Hat Update for pki-core (RHSA-2021:0851)

[239195](#) Red Hat Update for pki-core (RHSA-2021:0975)

[239196](#) Red Hat Update for pki-core:10.6 (RHSA-2021:0966)

[239239](#) Red Hat Update for pki-core:10.6 (RHSA-2021:1263)

[257068](#) CentOS Security Update for pki-core (CESA-2021:0851)

[281480](#) Fedora Security Update for pki (FEDORA-2021-344dd24c84)

[281481](#) Fedora Security Update for pki (FEDORA-2021-6c412a4601)

[281505](#) Fedora Security Update for dogtag (FEDORA-2021-c0d6637ca5)

[352268](#) Amazon Linux Security Advisory for pki-core: ALAS2-2021-1630

[376912](#) Alibaba Cloud Linux Security Update for pki-core (ALINUX2-SA-2021:0014)

[376921](#) Alibaba Cloud Linux Security Update for pki-core:10.6 (ALINUX3-SA-2021:0020)

[670245](#) EulerOS Security Update for pki-core (EulerOS-SA-2021-1831)

[670314](#) EulerOS Security Update for pki-core (EulerOS-SA-2021-1910)

[670339](#) EulerOS Security Update for pki-core (EulerOS-SA-2021-1885)

[670869](#) EulerOS Security Update for pki-core (EulerOS-SA-2021-1910)

[940140](#) AlmaLinux Security Update for pki-core:10.6 (ALSA-2021:0966)

[960719](#) Rocky Linux Security Update for pki-core:10.6 (RLSA-2021:0966)

© [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](#)