CVE-2024-0914

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-0914
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-31 05:15:00 UTC
Updated	2024-04-02 19:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opencryptoki Project	Opencryptoki	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference
The Marvin Attack
2260407 – (CVE-2024-0914) CVE-2024-0914 opencryptoki: timing side-channel in handling of RSA PKCS#1 v1.5 padded ciphertexts (Marvin
RHSA-2024:1239
RHSA-2024:1608
cve-details
RHSA-2024:1411
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

Legacy QID Mappings

161408	Oracle Enterprise Linux Security Update for opencryptoki (ELSA-2024-1239)
161460	Oracle Enterprise Linux Security Update for opencryptoki (ELSA-2024-1608)
243046	Red Hat Update for opencryptoki (RHSA-2024:1239)
243095	Red Hat Update for opencryptoki (RHSA-2024:1411)
243162	Red Hat Update for opencryptoki (RHSA-2024:1608)
941617	AlmaLinux Security Update for opencryptoki (ALSA-2024:1239)
941636	AlmaLinux Security Update for opencryptoki (ALSA-2024:1608)
961148	Rocky Linux Security Update for opencryptoki (RLSA-2024:1608)