CVE-2004-0155

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2004-0155
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-06-01 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	The KAME IKE Daemon Racoon, when authenticating a peer during Phase 1, validates the X.509 certificate but does not v

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kame	Racoon	All	All	All	All
Application	Kame	Racoon	All	All	All	All

References

Reference
Repository / Oval Repository
Secunia - Advisories - KAME Racoon IKE Daemon RSA Signature Verification Vulnerability
US-CERT Vulnerability Note VU#552398
Racoon IKE Daemon Unauthorized X.509 Certificate Connection Vulnerability
redhat.com | Red Hat Support
20040407 CAN-2004-0155: The KAME IKE Daemon Racoon does not verify RSA Signatures during Phase 1, allows man-in-the-middle attack
'[product-security@apple.com: APPLE-SA-2004-05-03 Security Update 2004-05-03]' - MARC
MDKSA-2004:069
Gentoo Linux Documentation -- IPsec-Tools: authentication bug in racoon
SCOSA-2005.10
Advisories - Mandriva
Repository / Oval Repository

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.