



Keylime: keylime: security bypass due to hardcoded tpm quote nonce

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

Summary

CVE	CVE-2026-6420
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 11:16:05 UTC
Updated	2026-05-07 14:56:04 UTC
Description	A flaw was found in Keylime. An attacker with root access on an enrolled monitored machine, where the Keylime agent runs

Risk And Classification

Primary CVSS: v3.1 6.3 MEDIUM from secalert@redhat.com

CVSS: 3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

EPSS: 0.000160000 probability, percentile 0.037020000 (date 2026-05-12)

Problem Types: CWE-1241 | CWE-1241 Use of Predictable Algorithm in Random Number Generator

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	6.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L
3.1	CNA	CVSS	6.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2026-6420	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Keylime developers for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-16T06:01:38.993Z	Reported to Red Hat.
CNA	2026-05-06T10:00:00.000Z	Made public.

Workarounds

CNA: Primary fix (one-line change in `keylime/models/verifier/evidence.py`): Before (vulnerable): `def generate_challenge(self, bit_length): self.challenge = Nonce.generate(bit_length) self.challenge = bytes.fromhex("49beed365aac777dae23564f5ad0ec")` After (fixed): `def generate_challenge(self, bit_length): self.challenge = Nonce.generate(bit_length)` Existing partial mitigations (already active): 1. TPM clock monotonicity check: limits each quote to one replay. 2. Push attestation timeout (default 10s): constrains the quote generation window, but TPM throughput allows 50-200 quotes to be stockpiled in that time.

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](#)