NATIONAL CSIRT-CY

CVE-2025-4598 **01/06/2025**

Signal Handler Race Condition

Executive Summary

CVE-2025-4598 is a race condition vulnerability in systemd-coredump affecting multiple Linux distributions. It allows local attackers to exploit PID reuse and access core dumps of privileged (SUID) processes, potentially leaking sensitive data like password hashes or private keys. Though difficult to exploit, the impact on confidentiality is significant.

Analysis

The vulnerability hinges on timing—an attacker must rapidly replace a crashed SUID binary with a benign one while the system recycles the same PID. This race condition can lead to privilege information leakage without elevated rights. While the attack complexity is high and requires precise conditions, it underscores the broader risk of relying on PID-based assumptions in security-sensitive code. Patch updates have mitigated the issue by improving how core dumps are handled to prevent unauthorized access.

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-4598

Versions affected

- **Debian**:
  Affected: systemd prior to 252.38-1~deb12u1 (Debian 12 "Bookworm")
- **Red Hat Enterprise Linux (RHEL):**
  Affected versions not explicitly listed, but updates and advisories were issued for RHEL 8 and 9.
- **Amazon Linux 2023:**
  Vulnerable until patched in recent system updates.
- **Oracle Linux:**
  Inherits vulnerabilities from RHEL; affected similarly.

Solutions

To mitigate the vulnerability, update systemd to the latest patched version provided by your Linux distribution. The fix ensures core dumps are securely handled, preventing unauthorized access due to PID reuse. Disable systemd-coredump if not needed as an additional mitigation.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.