مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical “CrackArmor” Vulnerabilities in Linux AppArmor

Tracking #:432318596

Date:14-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that multiple critical vulnerabilities collectively named "CrackArmor" have been discovered in AppArmor, a widely used Mandatory Access Control (MAC) framework integrated into the Linux Kernel.

TECHNICAL DETAILS:

Multiple critical vulnerabilities collectively named "CrackArmor" have been discovered in AppArmor, a widely used Mandatory Access Control (MAC) framework integrated into the Linux Kernel.
The vulnerabilities allow unprivileged local users to escalate privileges to root, bypass security policies, escape container isolation, and cause kernel crashes. The flaws originate from kernel version 4.11 (released in 2017) and have remained undetected for nearly nine years.

The issue was discovered by the Qualys Threat Research Unit and publicly disclosed on 12 March 2026. According to asset telemetry from Qualys, more than 12.6 million enterprise Linux systems running AppArmor by default may be exposed.

These vulnerabilities impact systems where AppArmor is enabled, including distributions such as Ubuntu, Debian, and SUSE Linux Enterprise, which are widely used across data centers, cloud environments, Kubernetes clusters, and IoT platforms.

Technical Details
Affected Component

- **AppArmor**
- Integrated within the **Linux Kernel**

Affected Systems
Systems running AppArmor-enabled Linux distributions, including:

- **Ubuntu**
- **Debian**
- **SUSE Linux Enterprise**

Vulnerability Status

- CVE IDs: **Not yet assigned**
- Root cause: **Implementation flaws within AppArmor LSM**
- Introduced in: **Linux Kernel 4.11**

RECOMMENDATIONS:

- Patch Immediately: Apply vendor security updates for AppArmor components across all affected distributions.
- Monitor Profiles: Implement monitoring for unexpected changes in /sys/kernel/security/apparmor/ which may indicate active exploitation attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://blog.qualys.com/vulnerabilities-threat-research/2026/03/12/crackarmor-critical-apparmor-flaws-enable-local-privilege-escalation-to-root