

The Vigil@nce team watches public vulnerabilities impacting your computers, and then offers security solutions, a vigilance database and tools to fix them.

- ➔ Recent vulnerabilities
- ➔ Search by software
- ➔ Search for text
- ➔ RSS feed
- Vulnerability

## Vulnerability of Linux kernel: memory leak via ccp\_run\_aes\_gcm\_cmd()

### Synthesis of the vulnerability

An attacker can create a memory leak of the Linux kernel, via `ccp_run_aes_gcm_cmd()`, in order to trigger a denial of service.

- ✓ Vulnerable systems: [Linux](#).
- ✓ Severity of this threat: 1/4.
- ✓ Creation date: 15/09/2021.
- ✓ Références of this weakness: [CVE-2021-3744](#), [VIGILANCE-VUL-36416](#).

### Description of the vulnerability

The Linux kernel product allocates memory for its internal processing. However,...  
[Full bulletin, software filtering, emails, fixes, ...](#) ([Request your free trial](#))

This weakness alert impacts software or systems such as [Linux](#).

Our Vigil@nce team determined that the severity of this computer vulnerability note is low.

The trust level is of type confirmed by the editor, with an origin of user shell.

An attacker with a expert ability can exploit this [security bulletin](#).

### Solutions for this threat

Fixes for this vulnerability are not yet public.

[Full bulletin, software filtering, emails, fixes, ...](#) ([Request your free trial](#))

### Computer vulnerabilities tracking service

Vigil@nce provides a [networks vulnerabilities patch](#). The technology watch team tracks security threats targeting the computer system.

### Share this bulletin



