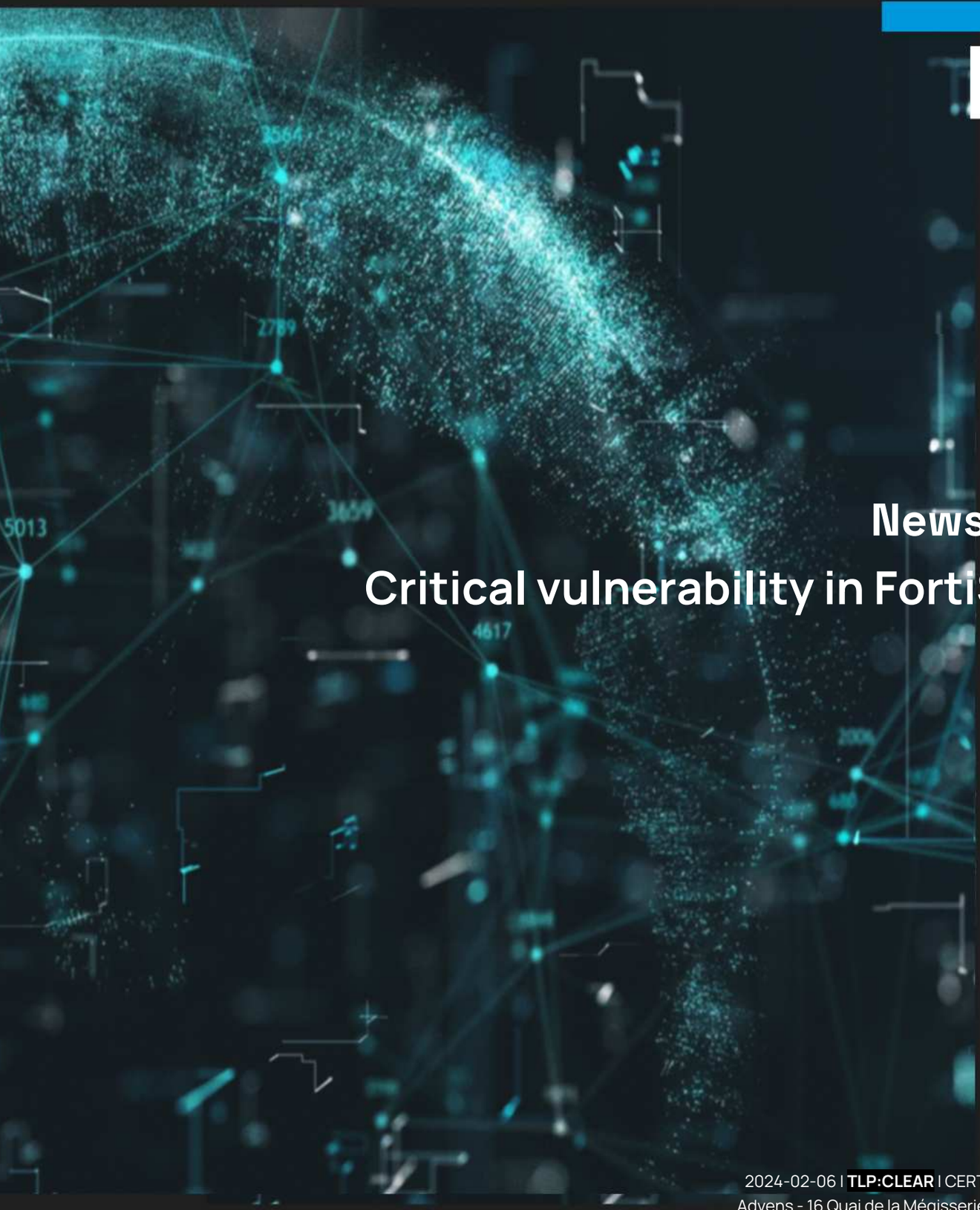
aDvens

Security for the greater good



Newscast

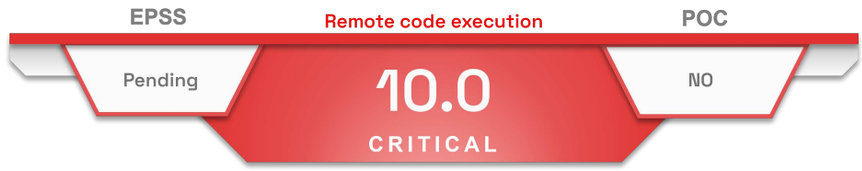
Critical vulnerability in FortiSIEM

2024-02-06 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Table of content

FortiSIEM - CVE-2024-23108/CVE-2024-23109



On 5 February 2024, two new critical Fortinet vulnerabilities were published. These vulnerabilities, identified as CVE-2024-23108 and CVE-2024-23109, are related to FortiSIEM's API.

An improper neutralisation of data sent to FortiSIEM's API allows a remote unauthenticated attacker to execute code via crafted requests.

Type of vulnerability

- **CWE-78**: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- FortiSIEM versions 7.1.0 through 7.1.1
- FortiSIEM versions 7.0.0 through 7.0.2
- FortiSIEM versions 6.7.0 through 6.7.8
- FortiSIEM versions 6.6.0 through 6.6.3
- FortiSIEM versions 6.5.0 through 6.5.2
- FortiSIEM versions 6.4.0 through 6.4.2

Recommendations

- Update FortiSIEM to version 6.7.9, 7.0.3, 7.1.3 or later. Fortinet has not confirmed that these versions patch the vulnerabilities.

Proof of concept

To date, no proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2024-23108
- https://www.cve.org/CVERecord?id=CVE-2024-23109
- https://www.fortiguard.com/psirt/FG-IR-23-130