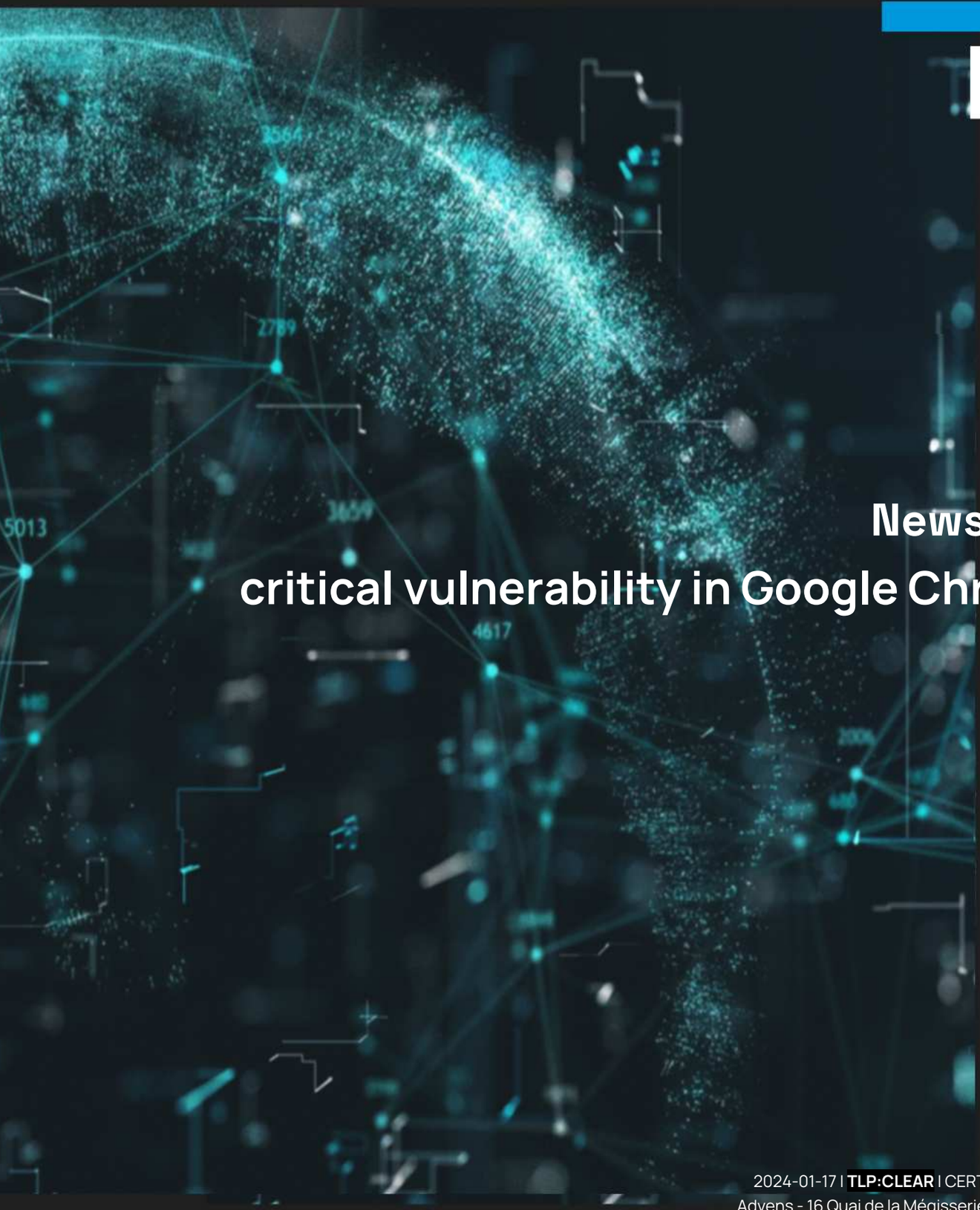
aDvens

Security for the greater good



Newscast
critical vulnerability in Google Chrome

2024-01-17 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Table of content

Google Chrome - CVE-2024-0519

On 16 January 2024, Google published a patch concerning 3 vulnerabilities in Chrome, including an exploited zero-day. The latter is due to an out-of-bounds memory access flaw in the V8 engine.

By persuading a victim to visit a specially crafted website, an attacker can execute arbitrary code or cause a denial of service.

This vulnerability is currently being exploited.

Type of vulnerability

- **CWE-125**: Out-of-bounds Read

Risks

- Remote Code Execution
- Denial of service

Severity (CVSS v3.1 base score)

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

Product impacted

Google Chrome :

- versions prior to 120.0.6099.224 on Windows and Linux
- versions prior to 120.0.6099.234 on macOS

Recommendations

- Update Google Chrome to version 120.0.6099.224 on Linux, 120.0.6099.224/225 on Windows and 120.0.6099.234 on macOS.
- Additional information is available in Google's Advisory.

Proof of concept

No proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2024-0519
- https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- https://www.bleepingcomputer.com/news/security/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/