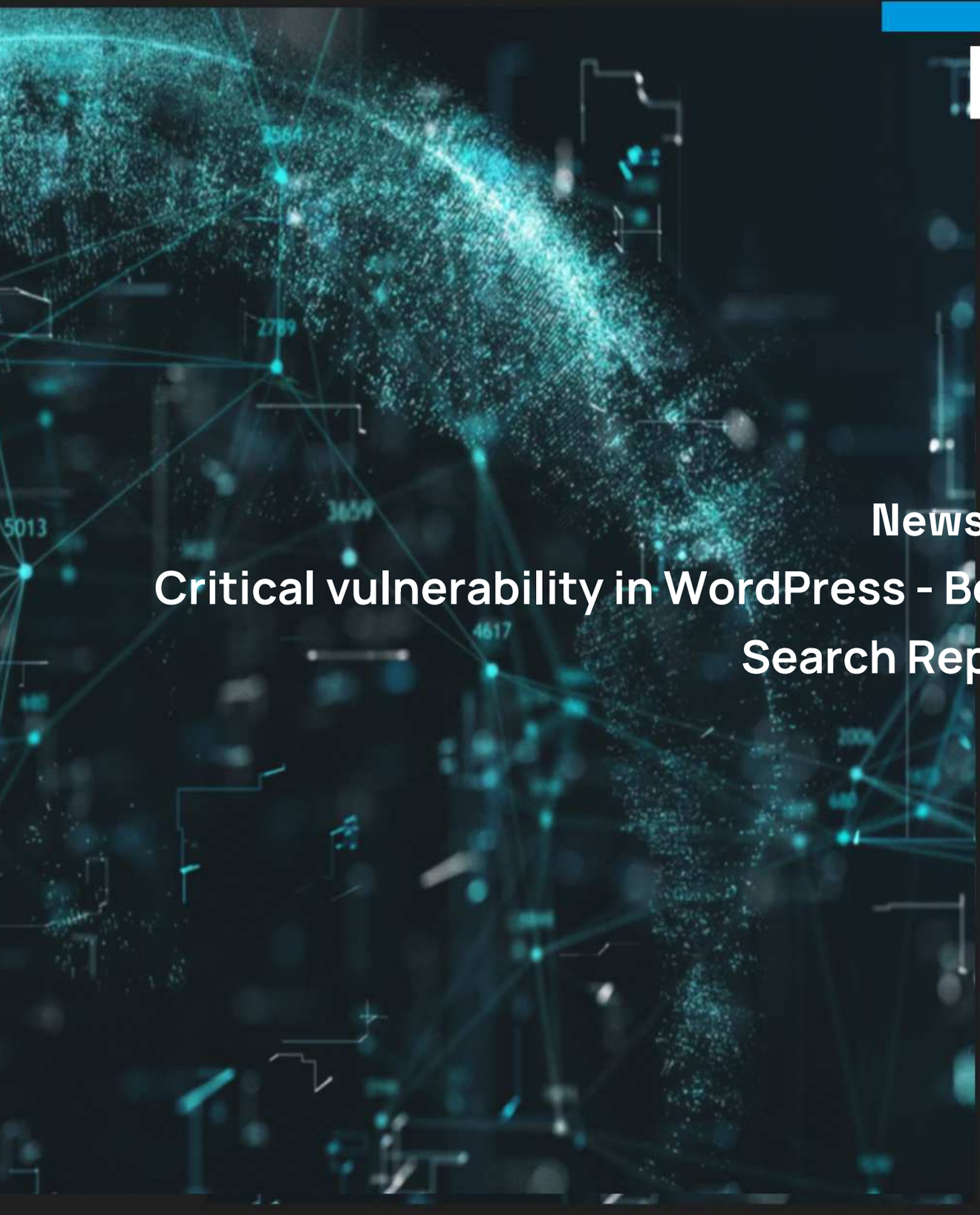
aDvens

Security for the greater good



Newscast

Critical vulnerability in WordPress - Better Search Replace

2024-01-25 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

WordPress - Better Search Replace - CVE-2023-6933

On 24 January 2024, Wordfence published a security advisory concerning the critical vulnerability CVE-2023-6933 in the *Better Search Replace* plugin for WordPress.

Better Search Replace is installed on over a million WordPress websites. This plugin is used to ease the migration of a database following a change of domain or server.

Security researcher Sam Pizzey identified an insecure deserialisation in the plugin, making it vulnerable to PHP object injections.

By sending specially crafted PHP requests, an unauthenticated attacker can delete files, steal sensitive data or execute arbitrary code.

This vulnerability is exploited.

Wordfence warned that it has blocked over 2,551 attempts to exploit this vulnerability in the last 24 hours.

Type of vulnerability

- **CWE-502**: Deserialization of Untrusted Data

Risks

- Remote code execution
- Sensitive data theft
- Abitrary files deletion

Severity (base score CVSS 3.1)

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

Impacted Products

- The WordPress plugin Better Search Replace version 1.4.4 and prior

Recommendations

- Update the Better Search Replace plugin to version 1.4.5 or later.
- Additional information is available in Wordfence's security advisory.

Proof of concept

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

Sources

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6933
- https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/better-search-replace/better-search-replace-144-unauthenticated-php-object-injection