aDvens

Security for the greater good

Newscast
critical vulnerability in PRIM'X

2023-12-14 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

PRIM'X **2**
CVE-2023-50444 ..... **2**
Type of vulnerability 2
Risk 2
Severity (base score CVSS 3.1) 2
Impacted Products 2
Recommendations 3
Proof of concept 3
SOURCES **4**

PRIM'X

On 14 December, 2023, the editor for encryption solutions for infrastructures, *Prim'x*, announces fixes for six vulnerabilities :

- CVE-2023-50439 score 5.3
- CVE-2023-50440 score 7.5
- CVE-2023-50441 score 4.8
- CVE-2023-50442 score 4.1
- CVE-2023-50443 score 4.0
- CVE-2023-50444 score 8.7

This bulletin focuses on the vulnerability CVE-2023-50444 which affects *ZED! Entreprise* for Windows.

CVE-2023-50444

Security researchers have discovered that .ZED container metadata is vulnerable to a brute force attack when the user's password is weak.

Exploitation of this flaw by a remote and unauthenticated attacker allows sensitive user information to be disclosed.

Type of vulnerability

- **CWE-200** : Exposure of Sensitive Information to an Unauthorized Actor
- **CWE-284** : Improper Access Control
- **CWE-266** : Incorrect Privilege Assignment

Risk

- Disclosure of information

Severity (base score CVSS 3.1)

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

Impacted Products

- *ZED! Enterprise* for Windows version prior to 2023.5, including versions Q.2020.1, Q.2020.2 and Q.2021.1 ;
- *ZED!* features in *ZONECENTRAL* for Windows version prior to 2023.5, including versions Q.2021.1 ;
- *ZED!* features in *ZEDMAIL* for Windows version prior to 2023.5 ;

Recommendations

The fixes

- *ZED! Enterprise* for Windows version Q.2020.3 (version validated by ANSSI)
- *ZED! Enterprise* for Windows version Q.2021.2 (version validated by ANSSI)
- *ZED! Enterprise* for Windows minimal version 2023.5
- *ZED!* features in *ZONECENTRAL* for Windows version Q.2021.2 (version validated by ANSSI)
- *ZED!* features in *ZONECENTRAL* for Windows minimal version 2023.5
- *ZED!* features in *ZEDMAIL* for Windows minimal version 2023.5

Editor security advisory

- Further information is available in the editor's security advisory

Specific recommendations from ANSSI

In addition to the deployment of patches, it is necessary to:

- Create new Zed! containers, old ones shall not be reused ;
- Enforce a strong password policy for user passwords (if the access list is password protected). reading the following documentation is recommended Multi-factor authentication and password recommendations ;
- Control access rights to zone files used by *ZoneCentral* and limit writing rights to *ZoneCentral* administrators only.

Proof of concept

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

Sources

CVE-2023-50444

- https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-1021/
- https://nvd.nist.gov/vuln/detail/CVE-2023-50444
- https://www.primx.eu/en/bulletins/security-bulletin-23B30874/

PRIM'X

- https://www.primx.eu/en/bulletins/security-bulletin-23b30930/
- https://www.primx.eu/en/bulletins/security-bulletin-23b3093b/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30874/
- https://www.primx.eu/en/bulletins/security-bulletin-23b3093a/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30931/
- https://www.primx.eu/en/bulletins/security-bulletin-23b30933/

ANSSI

- https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe