Security advisory

Schuhfried <=V8.22.00 Pre-authentication backend info leak leading to PrivEsc

February, 2024

CVE-2023-38995
Release date: 01/02/2024
Department: POST Cyberforce
Khalid ESSALMI

Vulnerability summary

Product	Schuhfried
Product homepage	https://www.schuhfried.com/
Affected product versions	V8.22.00
Severity	Critical: CVSS v3.1 score - 9.8
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
MITRE ATT&CK	T1068, T1190
OWASP	OWASP 2017-A3
CWE	CWE-259,
Workarounds	No workarounds available
Fixed product versions	N/A

Validated impact:

- Adding, deleting or updating an account/data;
- Escalate the privileges;
- Access to tests' reports;

Timeline

Date	Action
18 April 2023	Vulnerability identification, exploitation and impact validation
05 Mai 2023	Vendor notified and acknowledged the vulnerability
18 August 2023	CVE-2023-38995 assigned by MITRE
01 February 2023	Advisory publicly released by POST Cyberforce (no feedback from the vendor)

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38995
- https://attack.mitre.org/techniques/T1190/
- https://attack.mitre.org/techniques/T1068/
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
- https://cwe.mitre.org/data/definitions/259.html

Product description

Schuhfried is a multi environments platform, which segregation is normally implemented between them, which means that users of an environment must not access users' data of another one. Moreover, in each environment, four security levels are implemented:

- Level 0 : This is the highest security level on the application, permits to access all the application features;
- Level 1 : Access to all users data and tests results. No access to the settings of VTS;
- Level 2 : The users of this level are limited to administering and scoring the tests;
- Level 3 : Users of this level could only show tests' results. The users of Schuhfried application mainly used a heavy client, in addition to a web service to enable their accounts.

Advisory

Schuhfried <=V8.22.00 application allows users to gain unauthorized access to the backend MSSQL database by retrieving its password. This can be done by everyone, even without authentication. Which could lead to severe consequences, such as modifying or deleting sensitive data, adding new accounts, or escalating the privileges.

Vulnerability description

Configuration files accessible via URLs without authentication, which are contain the credentials of the database.

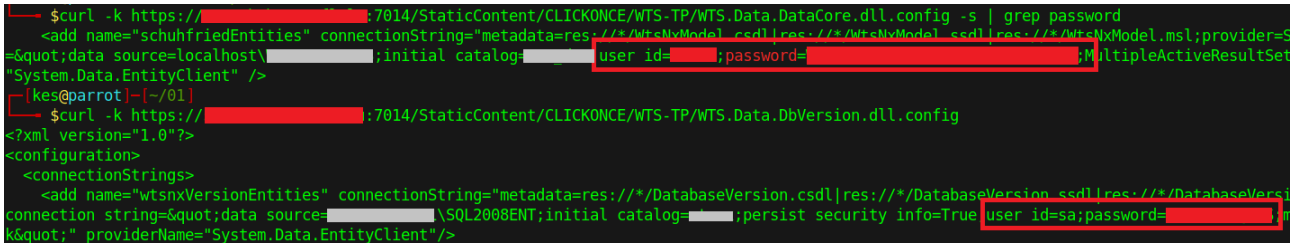
Examples of configuration files:

- https://[domain]:[port]/StaticContent/CLICKONCE/WTS-TP/WTS.Data.DataCore.dll.config
- https://[domain]:[port]/StaticContent/CLICKONCE/WTS-TP/WTS.Data.dbVersion.dll.config

Vulnerable endpoints:

- GET /StaticContent/CLICKONCE/WTS-TP/WTS.Data.DataCore.dll.config HTTP/1.1
- GET /StaticContent/CLICKONCE/WTS-TP/WTS.Data.dbVersion.dll.config HTTP/1.1

Proof of concept



Recommendation

Contact VENDOR to receive an updated version.