Security advisory

Pre-authenticated SQL Injection vulnerability in MyHorus V 4.3.5

July, 2024

CVE-2024-28297
Release date: 17/06/2024
Department: POST Cyberforce
PIANEZZOLA Thomas
ESSALMI Khalid

Vulnerability summary

Product	MyHorus
Product homepage	https://www.azursoft.com/
Affected product versions	4.3.5
Severity	Medium: CVSS v4.0 score - 6.9
CVSS v4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
MITRE ATT&CK	T1190
OWASP	OWASP A03:2021
CWE	CWE-89
Workarounds	No workarounds available
Fixed product versions	N/A

Validated impact:

MyHorus database exfiltration.

Timeline

Date	Action
09 February 2024	Vulnerability identification, exploitation and impact validation
27 February 2024	Vendor notified via en email, but no response.
27 February 2024	CVE Request via MITRE web site.
29 April 2024	CVE-2024-28297 assigned by MITRE.
30 April 2024	Vendor informed about the assigned CVE id, but no response.
07 Mai 2024	A third email sent to the vendor, but no response.
17 July 2024	Communication to the Vendor about the public release.
17 July 2024	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28297
- https://attack.mitre.org/techniques/T1190/
- https://owasp.org/Top10/A03_2021-Injection/
- https://cwe.mitre.org/data/definitions/89.html

Product description

MYHorus is software solution for monitoring centers, remote assistance, and lift call centers. Horus has several modules:

- Real-time monitoring of fundamental operating indicators;
- After-sales service;
- Geolocation of alarms, vehicles and security agents;
- Numerous connectors with professional security software;
- Supervision of interventions;
- ...

Advisory

A parameter in the MYHorus application was vulnerable to Pre-authenticated SQL Injection, allowing an attacker to extract DBMS data.

This issue affects the latest version of the MYHorus application (version 4.3.5).

Vulnerability description

For obvious reason no more technical details could be provided on this advisory.

Recommendation

Contact the VENDOR (no fix available at this time).