VDB-307195 · CVE-2025-4218 · ISSUE 20

HANDREW BROWSERPILOT UP TO 0.2.51 GPT_SELENIUM_AGENT.PY GPTSELENIUMAGENT INSTRUCTIONS CODE INJECTION

A vulnerability was found in handrew browserpilot up to 0.2.51. It has been declared as critical. Affected by this vulnerability is the function `GPTSeleniumAgent` of the file *browserpilot/browserpilot/agents/gpt_selenium_agent.py*. The manipulation of the argument `instructions` with an unknown input leads to a code injection vulnerability. The CWE definition for the vulnerability is CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2025-4218. The exploitation appears to be easy. Attacking locally is a requirement. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1059 according to MITRE ATT&CK.

It is possible to download the exploit at github.com. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Vendor

- handrew

Name

- browserpilot

Version

- 0.2.0
- 0.2.1
- 0.2.2
- 0.2.3
- 0.2.4
- 0.2.5
- 0.2.6
- 0.2.7
- 0.2.8
- 0.2.9
- 0.2.10
- 0.2.11
- 0.2.12
- 0.2.13
- 0.2.14
- 0.2.15

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 5.0

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 5.3
CNA Vector: 🔒

CVSSv2

[redacted]

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

[redacted]

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/02/2025		Advisory disclosed
05/02/2025	+0 days	VulDB entry created
05/03/2025	+1 days	VulDB entry last update

Sources

Advisory: 20
Status: Not defined

CVE: CVE-2025-4218 (🔒)
GCVE (CVE): GCVE-0-2025-4218
GCVE (VulDB): GCVE-100-307195
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 05/02/2025 03:00 PM
Updated: 05/03/2025 10:11 AM
Changes: 05/02/2025 03:00 PM (57), 05/03/2025 10:11 AM (30)
Complete: 🔍
Submitter: ybdesire
Cache ID: 5:279:101

Submit

Accepted

- Submit #562383: handrew browserpilot 0.0 Code Injection (by ybdesire)

Duplicate

- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.