COMMUNITY CONTENT

Submit #792653: AstrBotDevs AstrBot 4.22.1 Arbitrary Code Execution via Plugin Upload

Title	AstrBotDevs AstrBot 4.22.1 Arbitrary Code Execution via Plugin Upload
Description	AstrBot versions up to and including 4.22.1 allow authenticated users to achieve arbitrary code execution on the server by uploading a malicious plugin ZIP file via the /api/plugin/install-upload endpoint. The uploaded plugin's Python code is dynamically loaded via __import__() without any code signing verification, sandboxing, or content validation, allowing an attacker to execute arbitrary Python code in the context of the AstrBot server process.
Source	⚠ https://github.com/AstrBotDevs/AstrBot/issues/7168
User	Yu_Bao (UID 89348)
Submission	03/30/2026 05:27 AM (13 days ago)
Moderation	04/11/2026 10:50 AM (12 days later)
Status	Accepted
VulDB entry	356977 [AstrBotDevs AstrBot up to 4.22.1 install-upload Endpoint plugin.py install_plugin_upload File sandbox]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling