CVE-2020-15251

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15251
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-13 18:15:00 UTC
Updated	2021-11-18 16:58:00 UTC
Description	In the Channelmgnt plug-in for Sopel (a Python IRC bot) before version 1.0.3, malicious users are able to op/voice and take

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miraheze	Channelmgnt	All	All	All	All
Application	Miraheze	Channelmgnt	All	All	All	All
Application	Mirahezebots	Channelmgnt	All	All	All	All

References

Reference
sopel-plugins.channelmgnt · PyPI
[SECURITY] Actually fix by RhinosF1 · Pull Request #3 · MirahezeBots/sopel-channelmgnt · GitHub
⚓ T117 [CVE-2020-15251] makemodechange failed to check access on restricted changes for self actions allowing ACL bypass {Version 9.0.
Privilege Escalation issue in makemodechange self action logic · Advisory · MirahezeBots/MirahezeBots · GitHub
☆ Summary
Privilege Escalation issue in makemodechange self action logic · Advisory · MirahezeBots/sopel-channelmgnt · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980063 Python (pip) Security Update for sopel_plugins.channelmgnt (GHSA-j257-jfvv-h3x5)