



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.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)