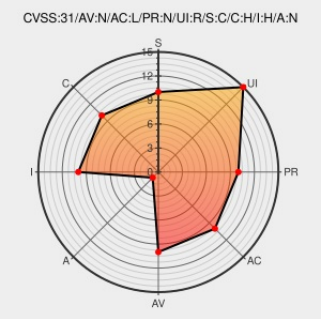
CVE-2020-15271

Published on: 10/26/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-15271 - advisory for GHSA-c84h-w6cr-5v8q

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Lookatme from Lookatme Project contain the following vulnerability:

In lookatme (python/pypi package) versions prior to 2.3.0, the package automatically loaded the built-in "terminal" and "file_loader" extensions. Users that use lookatme to render untrusted markdown may have malicious shell commands automatically run on their system. This is fixed in version 2.3.0. As a workaround, the `lookatme/contrib/terminal.py` and `lookatme/contrib/file_loader.py` files may be manually deleted. Additionally, it is always recommended to be aware of what is being rendered with lookatme.

CVE-2020-15271 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **d0c-s4vage** - **lookatme** version **< 2.3.0**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

CVE References

Description	Tags	Link
lookatme · PyPI	Release Notes Third Party Advisory pypi.org text/html	MISC pypi.org/project/lookatme/#history
Markdown-supplied Shell Command Execution · Advisory · d0c-s4vage/lookatme · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/d0c-s4vage/lookatme/security/advisories/GHSA-c84h-w6cr-5v8q
Adds warnings about loading extensions by d0c-s4vage · Pull Request #110 · d0c-s4vage/lookatme · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/d0c-s4vage/lookatme/pull/110
Release v2.3.0 · d0c-s4vage/lookatme · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/d0c-s4vage/lookatme/releases/tag/v2.3.0
Merge pull request #110 from d0c-s4vage/feature/109-extension_warnings · d0c-s4vage/lookatme@72fe36b · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/d0c-s4vage/lookatme/commit/72fe36b784b234548d49dae60b840c37f0eb8d84

Related QID Numbers

983215 Python (pip) Security Update for lookatme (GHSA-c84h-w6cr-5v8q)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lookatme Project	Lookatme	All	All	All	All
Application	Lookatme Project	Lookatme	All	All	All	All

cpe:2.3:a:lookatme_project:lookatme:*:*:*:*:*:*:*:*:

cpe:2.3:a:lookatme_project:lookatme:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report