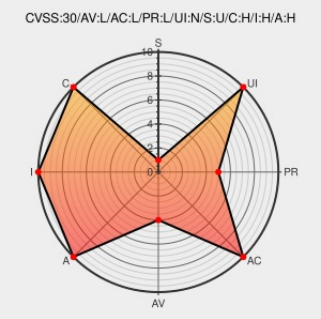
CVE-2018-6353

Published on: 01/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6353

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



Certain versions of Electrum from Electrum contain the following vulnerability:

The Python console in Electrum through 2.9.4 and 3.x through 3.0.5 supports arbitrary Python code without considering (1) social-engineering attacks in which a user pastes code that they do not understand and (2) code pasted by a physically proximate attacker at an unattended workstation, which makes it easier for attackers to steal Bitcoin via hook code that runs at a later time when the wallet password has been entered, a different vulnerability than CVE-2018-1000022.

CVE-2018-6353 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
why is it possible to execute arbitrary system commands via python code	Exploit	MISC

why is it possible to execute arbitrary system commands via python code through the electrum (Qt) console · Issue #3678 · spesmilo/electrum · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/spesmilo/electrum/issues/3678
Add a warning about harmful code to the Qt console by bauerj · Pull Request #3700 · spesmilo/electrum · GitHub	Third Party Advisory github.com text/html	MISC github.com/spesmilo/electrum/pull/3700

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Electrum	Electrum	3.0.0	All	All	All
Application	Electrum	Electrum	3.0.1	All	All	All
Application	Electrum	Electrum	3.0.2	All	All	All
Application	Electrum	Electrum	3.0.3	All	All	All
Application	Electrum	Electrum	3.0.5	All	All	All
Application	Electrum	Electrum	3.0.0	All	All	All
Application	Electrum	Electrum	3.0.1	All	All	All
Application	Electrum	Electrum	3.0.2	All	All	All
Application	Electrum	Electrum	3.0.3	All	All	All
Application	Electrum	Electrum	3.0.5	All	All	All
Application	Electrum	Electrum	All	All	All	All

cpe:2.3:a:electrum:electrum:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:electrum:electrum:3.0.5:*:*:*:*:*:*:*

cpe:2.3:a:electrum:electrum:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→