



CVE-2021-43839

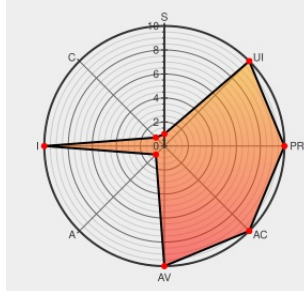
Published on: Not Yet Published

Last Modified on: 01/05/2022 03:10:00 PM UTC

CVE-2021-43839 - advisory for GHSA-f854-hpxv-cw9r

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Cronos](#) from [Crypto](#) contain the following vulnerability:

Cronos is a commercial implementation of a blockchain. In Cronos nodes running versions before v0.6.5, it is possible to take transaction fees from Cosmos SDK's FeeCollector for the current block by sending a custom crafted MsgEthereumTx. This problem has been patched in Cronos v0.6.5. There are no tested workarounds. All validator node

operators are recommended to upgrade to Cronos v0.6.5 at their earliest possible convenience.

CVE-2021-43839 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [crypto-org-chain](#) - **cronos** version < 0.6.5

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Drainage of FeeCollector's Block Transaction Fees · Advisory · crypto-org-chain/cronos · GitHub	github.com text/html	CONFIRM github.com/crypto-org-chain/cronos/security/advisories/GHSA-f854-hpxv-cw9r
Problem: MsgEthereumTx wrapping tx without the extension option is no... · crypto-org-chain/cronos@150ef23 · GitHub	github.com text/html	MISC github.com/crypto-org-chain/cronos/commit/150ef237b37ac28c8136e1c0f494932860b9ebe8
Problem: MsgEthereumTx wrapping tx without the extension option is not rejected by yihuang · Pull Request #270 · crypto-org-chain/cronos · GitHub	github.com text/html	MISC github.com/crypto-org-chain/cronos/pull/270

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crypto	Cronos	All	All	All	All
Application	Crypto	Ethermint	All	All	All	All
Application	Crypto	Ethermint	All	All	All	All
Application	Crypto	Evmos	All	All	All	All
cpe:2.3:a:crypto:cronos:*****:						
cpe:2.3:a:crypto:ethermint:*****:						
cpe:2.3:a:crypto:ethermint:*****:						
cpe:2.3:a:crypto:evmos:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43839 : Cronos is a commercial implementation of a blockchain. In Cronos nodes running versions before v0.... twitter.com/i/web/status/1...	2021-12-21 16:57:17
/r/netcve	CVE-2021-43839	2021-12-21 17:38:05

[← Previous ID](#)

[Next ID →](#)

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](#)