

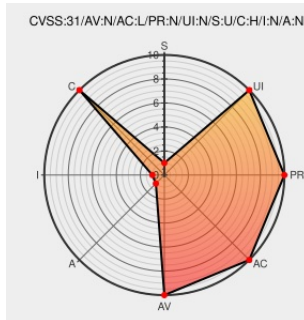


CVE-2020-12607

Published on: 06/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12607

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

Certain versions of [Fastecdsa](#) from [Fastecdsa Project](#) contain the following vulnerability:

An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s^{-1} , the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail.

CVE-2020-12607 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Update CHANGELOG.md · AntonKueltz/fastecdsa@4a16dae	Issue Tracking Patch	CONFIRM github.com/AntonKueltz/fastecdsa/commit/4a16daeaf139be20654ef58a9fe4c79dc0

Third Party Advisory
github.com
text/html

```
Patch
Third Party Advisory
github.com
text/html
```

 CONFIRM

- Exploit
- Third Party Advisory
- github.com
- text/html


```
Patch
Third Party Advisory
github.com
text/html
```

 CONFIRMcomment@cve.report

[980443](#) Python (pip) Security Update for fastecdsa (GHSA-56wv-2wr9-3h9r)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fastecdsa Project	Fastecdsa	All	All	All	All
Application	Fastecdsa Project	Fastecdsa	All	All	All	All
cpe:2.3:a:fastecdsa_project:fastecdsa:*****.*.*.						
cpe:2.3:a:fastecdsa_project:fastecdsa:*****.*.*.						

[← Previous ID](#)

Next ID→