



CVE-2020-17478

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-17478
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-10 18:15:00 UTC
Updated	2020-08-12 15:31:00 UTC
Description	ECDSA/EC/Point.pm in Crypt::Perl before 0.33 does not properly consider timing attacks against the EC point multiplication

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	P5-crypt-perl Project	P5-crypt-perl	All	All	All	All
Application	P5-crypt-perl Project	P5-crypt-perl	All	All	All	All

References

Reference	Source	Link	Tags
Comparing 0.32...0.33 · FGasper/p5-Crypt-Perl · GitHub	MISC	github.com	Patch, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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