



CVE-2019-10764

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

Summary

CVE	CVE-2019-10764
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-18 22:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In elliptic-php versions prior to 1.0.6, Timing attacks might be possible which can result in practical recovery of the long-term

Risk And Classification

Problem Types: CWE-203

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Simplito	Elliptic-php	All	All	All	All
Application	Simplito	Elliptic-php	All	All	All	All

References

Reference	Source	Link	Tags
Timing Attack in simplito/elliptic-php Snyk	MISC	snyk.io	Third Party Advisory
minerva.crocs.fi.muni.cz	MISC	minerva.crocs.fi.muni.cz	Exploit, 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.

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](#).

Free CVE JSON API cve.report/api

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