CVE-2012-2330

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-2330
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-13 23:55:00 UTC
Updated	2023-02-13 04:33:00 UTC
Description	The Update method in src/node_http_parser.cc in Node.js before 0.6.17 and 0.7 before 0.7.8 does not properly check the le

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodejs	Nodejs	0.7.0	All	All	All
Application	Nodejs	Nodejs	0.7.1	All	All	All
Application	Nodejs	Nodejs	0.7.2	All	All	All
Application	Nodejs	Nodejs	0.7.3	All	All	All
Application	Nodejs	Nodejs	0.7.4	All	All	All
Application	Nodejs	Nodejs	0.7.5	All	All	All
Application	Nodejs	Nodejs	0.7.6	All	All	All
Application	Nodejs	Nodejs	0.7.7	All	All	All
Application	Nodejs	Nodejs	All	All	All	All
Application	Nodejs	Nodejs	0.7.0	All	All	All
Application	Nodejs	Nodejs	0.7.1	All	All	All
Application	Nodejs	Nodejs	0.7.2	All	All	All
Application	Nodejs	Nodejs	0.7.3	All	All	All
Application	Nodejs	Nodejs	0.7.4	All	All	All
Application	Nodejs	Nodejs	0.7.5	All	All	All
Application	Nodejs	Nodejs	0.7.6	All	All	All
Application	Nodejs	Nodejs	0.7.7	All	All	All

References

Reference	Source	Link	Tags
typo in node_http_parser · c9a231d · joyent/node · GitHub	CONFIRM	github.com	Exploi
Security Advisory SA49066 - Node.js HTTP Parser Information Disclosure Vulnerability - Secunia	SECUNIA	secunia.com	Vendo
Version 0.6.17 (stable)	CONFIRM	blog.nodejs.org	
oss-security - Re: CVE request: node.js <0.6.17/0.7.8 HTTP server information disclosure	MLIST	www.openwall.com	
typo in node_http_parser · 7b3fb22 · joyent/node · GitHub	CONFIRM	github.com	Exploi
support.f5.com/csp/article/K99038439	MISC	support.f5.com	
support.f5.com/csp/article/K99038439	CONFIRM	support.f5.com	
oss-security - CVE request: node.js <0.6.17/0.7.8 HTTP server information disclosure	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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