CVE-2013-2028

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

Summary

CVE	CVE-2013-2028
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-20 03:37:00 UTC
Updated	2021-11-10 15:59:00 UTC
Description	The ngx_http_parse_chunked function in http/ngx_http_parse.c in nginx 1.3.9 through 1.4.0 allows remote attackers to caus

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F5	Nginx	All	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Application	Nginx	Nginx	All	All	All	All

References

Reference	Sour
Analysis of nginx 1.3.9/1.4.0 stack buffer overflow and x64 exploitation (CVE-2013-2028) : VNSECURITY / CLGT TEAM	MISC
nginx.org/download/patch.2013.chunked.txt	MISC
[nginx-announce] nginx security advisory (CVE-2013-2028)	MLIS
Malformed Request	BID
About Secunia Research | Flexera	SECU
Exploit module for nginx chunked stack buffer overflow. by linuxgeek247 · Pull Request #1834 · rapid7/metasploit-framework · GitHub	MISC
Nginx 1.3.9 / 1.4.0 Denial Of Service ≈ Packet Storm	MISC
Gentoo Linux Documentation -- nginx: Multiple vulnerabilities	GENT
93037	OSVD
[SECURITY] Fedora 19 Update: nginx-1.4.1-1.fc19	FEDO

CVE Program record	CVE.(
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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