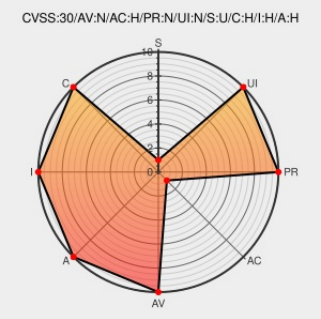
CVE-2019-9053

Published on: 03/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9053

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cms Made Simple from Cmsmadesimple contain the following vulnerability:

An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL injection via the m1_idlist parameter.

CVE-2019-9053 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CMS Made Simple < 2.2.10 - SQL Injection - PHP webapps Exploit	Exploit, Third Party Advisory, VDB Entry, www.exploit-db.com, Proof of Concept	EXPLOIT-DB 46635

	text/html	
Blog : : CMS Made Simple	Release Notes Vendor Advisory www.cmsmadesimple.org text/html	CONFIRM www.cmsmadesimple.org/2019/03/Announcing-CMS-Made-Simple-v2.2.10-Spuzzum
CMS Made Simple™ Newsletter - News	Release Notes Vendor Advisory newsletter.cmsmadesimple.org text/html	MISC newsletter.cmsmadesimple.org/w/89247Qog4jCRCuRinvhsofwg
CMS Made Simple SQL Injection ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/152356/CMS-Made-Simple-SQL-Injection.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cmsmadesimple	Cms Made Simple	2.2.8	All	All	All
Application	Cmsmadesimple	Cms Made Simple	2.2.8	All	All	All

cpe:2.3:a:cmsmadesimple:cms_made_simple:2.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:cmsmadesimple:cms_made_simple:2.2.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@kubeworm	@cy4053 @0xValkyrie @johnjhacking gitlab.com/kubeworm/Tools… here's a fun one for you. A POC that a previously "patche… twitter.com/i/web/status/1…	2021-06-26 16:01:32
@SecurityCTF	HTB - Writeup - Understanding CVE-2019-9053 reddit.com/r/securityCTF/… #security #ctftime #ctf	2021-10-02 16:00:04
@_r_netsec	Understanding CVE-2019-9053 tpetersonkth.github.io/cve/2021/10/02…	2021-10-10 16:43:07
@CybrXx0	Understanding CVE-2019-9053 via /r/netsec ift.tt/302nblV #cybersecurity #netsec #news	2021-10-10 16:59:38
@aufzayed	CVE-2019-9053 analysis #pentest #bugbounty #cybersecurity tpetersonkth.github.io/cve/2021/10/02…	2021-10-10 17:33:09
@Myinfosecfeed	New post: "Understanding CVE-2019-9053" ift.tt/3By1CI2	2021-10-10 17:48:10

@KeoXes	Understanding CVE-2019-9053: ift.tt/3By1CI2 #follow & #RT #cybersecurity #infosec	2021-10-10 22:33:08
@axcheron	CVE-2019-9053 - CMS Made Simple tpetersonkth.github.io/cve/2021/10/02… #CVE	2021-10-11 10:48:00
@InfoSec_Pom	Blogs, social media, Reddit, and more! freethreatintel.com tpetersonkth.github.io/cve/2021/10/02… CVE-2019-9053 | CVE Analyses #TTPs #malware	2021-10-11 13:03:19
@InfoSecIrvin	CVE-2019-9053 | CVE Analyses tpetersonkth.github.io/cve/2021/10/02…	2021-10-11 15:24:20
@techadversary	Understanding CVE-2019-9053 reddit.com/r/netsec/comme… https://t.co/zqjFkGSOjc	2021-10-31 03:11:34
@reverseame	Understanding CVE-2019-9053 tpetersonkth.github.io/cve/2021/10/02…	2021-11-03 16:58:06
/r/cybersecurity	Exploiting CVE-2019-9053 and vim editor privilege escalation | TryHackMe Simple CTF	2021-02-20 14:13:23
/r/Information_Security	Exploiting CVE-2019-9053 and vim editor privilege escalation | TryHackMe Simple CTF	2021-02-20 13:47:10
/r/securityCTF	HTB - Writeup - Understanding CVE-2019-9053	2021-10-02 12:48:10
/r/Information_Security	Understanding CVE-2019-9053	2021-10-10 16:36:43
/r/netsec	Understanding CVE-2019-9053	2021-10-10 16:36:37
/r/cybersecurity	Understanding CVE-2019-9053	2021-10-10 16:32:25
/r/hacking	Understanding CVE-2019-9053	2021-10-10 16:30:01

← Previous ID

Next ID→