



SSRF via Host Header Spoofing in Custom Slash Commands

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2026-6333
State	PUBLISHED
Assigner	Mattermost
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-18 09:16:23 UTC
Updated	2026-05-18 09:16:23 UTC
Description	Mattermost versions 11.5.x <= 11.5.1, 10.11.x <= 10.11.13 fail to validate the Host header when constructing response URI

Risk And Classification

Primary CVSS: v3.1 3.5 LOW from responsiblydisclosure@mattermost.com

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:N

Problem Types: CWE-918 | CWE-918 CWE-918: Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	responsiblydisclosure@mattermost.com	Secondary	3.5	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:N
3.1	CNA	CVSS	3.5	LOW	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	High
Privileges Required	Low
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity	Low

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:L/A:N



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mattermost	Mattermost	affected 11.5.0 11.5.1 semver	Not specified
CNA	Mattermost	Mattermost	affected 10.11.0 10.11.13 semver	Not specified
CNA	Mattermost	Mattermost	unaffected 11.6.0	Not specified
CNA	Mattermost	Mattermost	unaffected 11.5.2	Not specified
CNA	Mattermost	Mattermost	unaffected 10.11.14	Not specified

References

Reference	Source	Link	Tags
mattermost.com/security-updates	responsibledisclosure@mattermost.com	mattermost.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Juho Forsén (en)

Additional Advisory Data

Solutions

CNA: Update Mattermost to versions 11.6.0, 11.5.2, 10.11.14 or higher.

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