

CVE-2017-6327

Symantec Messaging Gateway Remote Code Execution Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

The Symantec Messaging Gateway before 10.6.3-267 can encounter an issue of remote code execution, which describes a situation whereby an individual may obtain the ability to execute commands remotely on a target machine or in a target process. In this type of occurrence, after gaining access to the system, the attacker may attempt to elevate their privileges.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.359 98.5th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.359 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
message gateway	< 10.6.3-267	10.6.3-267	NVD

Sources

Vendor guidance github.com/advisories/GHSA-x45p-q5pf-h9jx

Additional guidance symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20170810_00

NVD nvd.nist.gov/vuln/detail/CVE-2017-6327

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-15388

Current data evulnable.com/vulnerability-management/cve/CVE-2017-6327

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.