

CVE-2024-11182

MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability

CISA KEV since May 19, 2025

Actively exploited

An XSS issue was discovered in MDaemon Email Server before version 24.5.1c. An attacker can send an HTML e-mail message with JavaScript in an img tag. This could allow a remote attacker to load arbitrary JavaScript code in the context of a webmail user's browser window.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V4.0 5.3 Medium · NVD	EPSS 0.314 98.3rd percentile · FIRST	CISA DEADLINE Jun 9, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.314 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
mdaemon	< 24.5.1	24.5.1	NVD

Sources

Vendor guidance	files.mdaemon.com/mdaemon/beta/RelNotes_en.html	Additional guidance	cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2024-11182
mdaemon.com	mdaemon.com/pages/downloads-critical-updates	NVD	nvd.nist.gov/vuln/detail/CVE-2024-11182
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-33681
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-11182		

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