

CISA Flags Fortinet FortiMail Path Traversal Vulnerability Under Active Exploitation



CISA has added a Fortinet FortiMail path traversal vulnerability to its Known Exploited Vulnerabilities Catalog following evidence of active exploitation in the wild.

- CVE-2026-104286 affecting Fortinet FortiMail has been added to CISA's Known Exploited Vulnerabilities Catalog due to active exploitation
- The vulnerability is a path traversal flaw that poses significant risk to enterprise environments
- US federal agencies are required to prioritize remediation under Binding Operational Directive 26-04
- CISA recommends all organizations adopt risk-based vulnerability management and prioritize KEV Catalog entries
- Organizations should check for potential compromise before applying patches to affected systems

Vulnerability Details

The US Cybersecurity and Infrastructure Security Agency has catalogued a **path traversal vulnerability** in Fortinet FortiMail as actively exploited. The flaw, tracked as CVE-2026-104286, has been added to CISA's Known Exploited Vulnerabilities Catalog based on confirmed evidence of exploitation by threat actors. Path traversal vulnerabilities represent a common attack vector that allows unauthorized access to files and directories outside intended boundaries, potentially granting attackers significant control over compromised systems.

Regulatory Context and Guidance

Under Binding Operational Directive 26-04, US federal civilian agencies must prioritize rapid remediation of high-risk vulnerabilities listed in the KEV Catalog, particularly those affecting publicly exposed assets that could grant total control post-exploitation. The directive also establishes requirements for agencies to assess whether systems were compromised before patches are applied. While this directive applies specifically to US federal agencies, CISA strongly encourages all organizations globally to adopt similar risk-based vulnerability management practices.

Implications for Saudi Organizations

Regulated institutions in the Kingdom operating Fortinet FortiMail infrastructure should treat this advisory as a priority signal. The presence of active exploitation indicates that threat actors possess working exploit code and are targeting vulnerable deployments. Organizations should immediately verify their exposure, assess potential compromise, and expedite patching activities in line with their vulnerability management frameworks and regulatory obligations under applicable Saudi cybersecurity controls.

CISA continues to update the KEV Catalog as new exploitation evidence emerges and accepts nominations for additional vulnerabilities through its formal submission process.

What to do now

1. Immediately inventory all Fortinet FortiMail deployments across your environment, including on-premises and cloud instances
2. Verify whether CVE-2026-104286 affects your specific FortiMail versions by consulting Fortinet security advisories
3. Conduct forensic assessment of potentially affected systems to detect indicators of compromise before applying patches
4. Apply vendor-supplied patches or mitigations as soon as possible, prioritizing publicly exposed instances
5. Review and update vulnerability management procedures to incorporate CISA KEV Catalog monitoring into regular security operations
6. Document remediation activities and timelines for audit purposes in accordance with NCA ECC or SAMA

cybersecurity framework requirements