

Fortinet FortiMail Path Traversal Vulnerability Enables Arbitrary File Write



A path traversal vulnerability in Fortinet FortiMail allows unauthenticated attackers to write arbitrary files on the system through crafted HTTP or HTTPS requests.

- CVE-2026-104286 affects Fortinet FortiMail with a path traversal and NULL byte neutralization flaw
- Unauthenticated attackers can write arbitrary files to the underlying system
- Exploitation occurs through specially crafted HTTP or HTTPS requests
- Organizations must apply vendor mitigations or discontinue product use if patches are unavailable
- Internet-exposed assets require immediate evaluation and prioritized remediation

Vulnerability Overview

Fortinet has disclosed a **path traversal vulnerability** in FortiMail, tracked as CVE-2026-104286, that permits unauthenticated attackers to write arbitrary files to the underlying system. The flaw combines path traversal with improper neutralization of NULL byte or NULL character handling, enabling exploitation through specially crafted HTTP or HTTPS requests without requiring authentication credentials.

The vulnerability represents a significant risk for organizations relying on FortiMail for email security, particularly those with internet-facing deployments. Successful exploitation could allow attackers to place malicious files in critical system directories, potentially leading to code execution, privilege escalation, or persistent compromise.

Remediation Guidance

Organizations are directed to apply mitigations in accordance with vendor instructions immediately. Where vendor patches or mitigations are not available, institutions should evaluate discontinuing use of the affected product, especially for internet-exposed instances. The advisory emphasizes the importance of evaluating each asset's internet exposure and prioritizing remediation based on risk.

Compliance Considerations

For regulated institutions in Saudi Arabia, this vulnerability requires prompt action under established vulnerability management frameworks. Organizations should document remediation activities, assess potential exposure of sensitive data, and review incident response procedures. Email security appliances often process confidential communications and personal data, making timely patching essential for regulatory compliance and data protection obligations.

What to do now

1. Identify all Fortinet FortiMail deployments within your environment, prioritizing internet-facing instances
2. Apply vendor-supplied patches or mitigations immediately in accordance with Fortinet security advisories
3. Evaluate discontinuing use of affected FortiMail systems if vendor mitigations are unavailable or cannot be applied promptly
4. Review logs for suspicious HTTP/HTTPS requests or unexpected file creation activity on FortiMail systems
5. Document remediation activities and timelines for compliance with NCA ECC vulnerability management requirements
6. Assess whether any sensitive data or regulated information may have been exposed and initiate incident response procedures if compromise is suspected