- Research

Research Center

Explore latest research and threat reports on emerging cyber threats.
- Outbreak Alerts
- Security Blog
- Threat Signal

- Services

Services

By Outbreak | By Solution | By Product

Protect

Counter measures across the security fabric for protecting assets, data and network.
- AI-Protect Security
- Anti-Botnet
- AntiMalware
- AntiSpam
- Application Control
- Intrusion Protection
- Operational Technology Security
- Sandbox Behavior Engine
- Web Application Security
- Web Filtering

Detect

Find and correlate important information to identify an outbreak.Find and correlate
- Anti-Recon and Anti-Exploit
- Cloud Threat Detection
- Endpoint Detection & Response
- Indicators of Compromise
- Outbreak Deception
- Outbreak Detection
- Security Automation

Respond

Develop containment techniques to mitigate impacts of security events.Develop containment
- Endpoint Detection and Response
- Endpoint Forensics
- Incident Response

Recover

Improve security posture and processes by implementing security awareness and training.

- Assessment Services
- NSE Training
- Security Awareness Training

Identify

Identify processes and assets that need protection.Identify processes and assets that

- Adversary Centric Intelligence
- Attack Surface Management
- Brand Protection
- Breach Attack Simulation
- Cloud Access Security
- Cloud Vulnerability
- DAST
- DevSecOps
- Endpoint Vulnerability
- IoT Device Detection
- Pen Testing
- Security Rating

Network Security

- Anti-Botnet
- Anti-Recon and Anti-Exploit
- Data Loss Prevention
- Indicators of Compromise
- Internet Services
- Intrusion Protection
- IP Geolocation
- Network Detection and Response
- Operational Technology Security
- Secure DNS
- Web Filtering

Cloud & Application Security

- AI-Protect Security
- Application Control
- Client Application Firewall
- Cloud Access Security
- Cloud Threat Detection
- Cloud Vulnerability
- Credential Stuffing Defense
- DAST
- Web Application Security

Endpoint Security

- AntiSpam
- AntiVirus

- Endpoint Detection & Response
- Endpoint Vulnerability
- IoT Device Detection
- Sandbox Behavior Engine
- Web Filtering

- **Security Operations**

  
  Security Operations icon
- Breach Attack Simulation
- DevSecOps
- Outbreak Deception
- Outbreak Detection
- Pen Testing
- Security Automation
- Security Rating

- FortiGate
- FortiAnalyzer
- FortiClient
- FortiWeb
- FortiADC
- FortiAuthenticator
- FortiCNP
- FortiDDoS

- FortiDeceptor
- FortiEDR
- FortiMail
- FortiNDR
- empty
- FortiPAM
- FortiPolicy
- FortiProxy
- FortiRecon
- FortiSandBox
- FortiSASE
- FortiSIEM
-

FortiTester

- FortiDAST
- FortiCNAPP
- FortiDLP

- empty
- AI-Protect Security
- Anti-Botnet
- AntiVirus
- Application Control
- Cloud Access Security
- Intrusion Protection
- IoT Device Detection
- IP Geolocation
- Operational Technology Security
- Sandbox Behavior Engine
- Secure DNS
- Security Rating
- Web Filtering
- Indicators of Compromise
- Outbreak Detection
- Security Automation
- Anti-Botnet
- Anti-Recon and Anti-Exploit
- AntiVirus
- Application Firewall
- Credential Stuffing Defense
- Endpoint Vulnerability
- Intrusion Protection
- Outbreak Detection
- Sandbox Behavior Engine
- Web Filtering
- Anti-Botnet
- AntiVirus
- Application Control
- Credential Stuffing Defense
- Fuzzy Webshell
- IP Geolocation
- Sandbox Behavior Engine
- Web Application Security
- Anti-Botnet
- AntiVirus

- Credential Stuffing Defense
- Intrusion Protection
- IP Geolocation
- Sandbox Behavior Engine
- Web Application Security
- Web Filtering
- IP Geolocation
- Anti-Botnet
- Data Loss Prevention
- IP Geolocation
- Vulnerability
- Anti-Botnet
- Anti-Recon and Anti-Exploit
- AntiVirus
- Intrusion Protection
- Outbreak Deception
- AntiVirus
- EndPoint Detection and Response
- Endpoint Vulnerability
- Indicators of Compromise
- Sandbox Behavior Engine
- Web Filtering
- AntiSpam
- AntiVirus
- Sandbox Behavior Engine
- Web Filtering
- Network Detection and Response
- Sandbox Behavior Engine
- AntiVirus
- Data Loss Prevention
- Anti-Botnet
- Application Control
- Anti-Botnet
- Application Control
- Industrial Security
- Sandbox Behavior Engine
- Digital Risk Protection
- AntiVirus
- Intrusion Protection
- Sandbox Behavior Engine
- Web Filtering
- Anti-Botnet
- AntiVirus
- Application Control
- Data Loss Prevention
- Endpoint Vulnerability
- Intrusion Protection
- Sandbox Behavior Engine
- Secure DNS
- Web Filtering
- Indicators of Compromise
- IP Geolocation
- Outbreak Detection
- Sandbox Behavior Engine

- Breach Attack Simulation
- DAST
- Cloud Threat Detection
- Cloud Vulnerability
- Data Loss Prevention

- Threat Intelligence

Threat Intelligence Center

Browse the FortiGuard Labs extensive encyclopedia and Threat Analytics.

- FortiGuard Encyclopedia
- Outbreak Threat Map
- Threat Actor Encyclopedia
- Threat Intel Search

- Support

Support Center

PSIRT Center | Product Support

Fortinet Product Security Incident Response Team (PSIRT) updates.

- Advisories
- PSIRT Blog
- PSIRT Contact
- Security Vulnerability Policy

Get the support whenever you need it.

- FortiCare Support
- Fortinet Community

- Resources

Resource Center

Learn about service status, publications and other available resources.

- 2025 Threat Landscape Report
- FortiGuard Sample Files
- MITRE ATT&CK Matrix
- NIST Cybersecurity Framework
- Outbreak Alert Annual Report
- Publications
- Security Best Practices

- About

About

FortiGuard Labs | Partners

AI-Powered Threat Intelligence for an Evolving Digital World.

- Contact Us
- Frequently Asked Questions
- Premium Services
- RSS Feeds

Leveraging cyber security industry partner relationships.
- Cyber Threat Alliance
- MITRE Engenuity

- search

Search FortiGuard

fortiguard-logo search

- Research
  - Outbreak Alerts
  - Security Blog
  - Threat Signal
- Services
  - Adversary Centric Intelligence
  - AI-Protect Security
  - Anti-Botnet
  - Anti-Recon and Anti-Exploit
  - AntiMalware
  - AntiSpam
  - Application Control
  - Assessment Services
  - Attack Surface Management
  - Brand Protection
  - Breach Attack Simulation
  - Cloud Access Security
  - Cloud Threat Detection
  - Cloud Vulnerability
  - DAST
  - DevSecOps
  - Endpoint Detection & Response
  - Endpoint Detection and Response
  - Endpoint Forensics
  - Endpoint Vulnerability
  - Incident Response
  - Indicators of Compromise
  - Intrusion Protection
  - IoT Device Detection
  - NSE Training
  - Operational Technology Security
  - Outbreak Deception
  - Outbreak Detection
  - Pen Testing
  - Sandbox Behavior Engine
  - Security Automation
  - Security Awareness Training
  - Security Rating
  - Web Application Security
  - Web Filtering
- Threat Intelligence
  - FortiGuard Encyclopedia
  - Outbreak Threat Map
  - Threat Actor Encyclopedia

- Threat Intel Search
- Resources
  - 2025 Threat Landscape Report
  - FortiGuard Sample Files
  - MITRE ATT&CK Matrix
  - NIST Cybersecurity Framework
  - Outbreak Alert Annual Report
  - Publications
  - Security Best Practices
- Support

PSIRT Center

- Advisories
- PSIRT Blog
- PSIRT Contact
- Security Vulnerability Policy

Product Support

- FortiCare Support
- Fortinet Community
- About

FortiGuard Labs

- Contact Us
- Frequently Asked Questions
- Premium Services
- RSS Feeds

Partners

- Cyber Threat Alliance
- MITRE Engenuity
- FORTINET

Search FortiGuard GO

virus logo PSIRT

OS command injection on endpoint

Summary

Multiple improper neutralization of special elements used in an OS Command vulnerabilities [CWE-78] in FortiSandbox may allow an authenticated attacker with at least read-only permission to execute unauthorized commands via crafted requests.

Version	Affected	Solution
FortiSandbox 4.4	4.4.0 through 4.4.3	Upgrade to 4.4.4 or above
FortiSandbox 4.2	4.2.1 through 4.2.6	Upgrade to 4.2.7 or above

Version	Affected	Solution
FortiSandbox 4.0	4.0.0 through 4.0.4	Upgrade to 4.0.5 or above
FortiSandbox 3.2	Not affected	Not Applicable

Acknowledgement

Internally discovered and reported by Adham El karn of Fortinet Product Security team.

Timeline

2024-04-09: Initial publication

IR Number	FG-IR-23-489
Published Date	Apr 9, 2024
Component	GUI
Severity	High
CVSSv3 Score	8.6
Impact	Execute unauthorized code or commands
CVE ID	CVE-2024-21755 CVE-2024-21756
Download	CVRF CSAF

Copyright © 2026 Fortinet, Inc. All Rights Reserved.