



# IBM Aspera Faspex Code Execution Vulnerability

## File transfer software exploited in the wild

<https://www.ibm.com/support/pages/node/6952319>

CVEs: [CVE-2022-47986](#)

IBM Aspera Faspex could allow a remote attacker to execute code on the system, caused by a YAML deserialization flaw. By sending a specially crafted obsolete API call, an attacker could exploit this vulnerability to execute arbitrary code on the system.

**Background**

IBM Aspera Faspex is a centralized transfer solution that enables users to exchange files with each other using an email-like workflow. In the recent weeks, Enterprise file transfer solutions are being targeted by attackers. A vulnerability in another file transfer software, GoAnywhere managed file transfer (MFT) software was also seen being targeted by the attackers. To read the full outbreak report go to <https://www.fortiguard.com/outbreak-alert/goanywhere-mft-rce>

**Announced**

January 18, 2023: IBM issued a patch  
<https://www.ibm.com/docs/en/aspera-faspex/4.4?topic=notes-release-aspera-faspex-442>

**Latest Developments**

February 21, 2023: CISA added the bug, CVE-2022-47986 to its catalog of known exploited vulnerabilities.

April 19, 2023: An Iranian nation-state actor observed exploiting CVE-2022-47986 for initial access.  
<https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/>

FortiGuard Labs recommends users to update the vulnerable version of IBM Aspera Faspex and apply latest patch as released by the vendor as soon as possible.

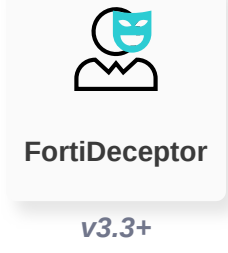
## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

### Reconnaissance

#### Lure

Detects and blocks attack attempts related to CVE-2022-47986 and prevents lateral movement on the network segment



v3.3+

#### Decoy VM

Detects and blocks attack attempts related to CVE-2022-47986 and prevents lateral movement on the network segment



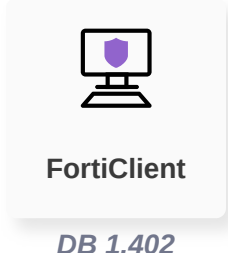
v3.3+

### Weaponization

### Delivery

#### Vulnerability

Detects vulnerable IBM Aspera Faspex related to CVE-2022-47986

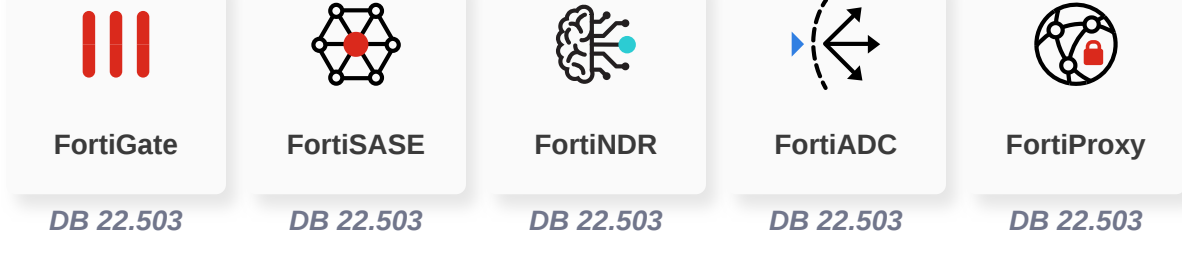


DB 1.402

### Exploitation

#### IPS

Detects and blocks attack attempts related to CVE-2022-47986



DB 22.503

DB 22.503

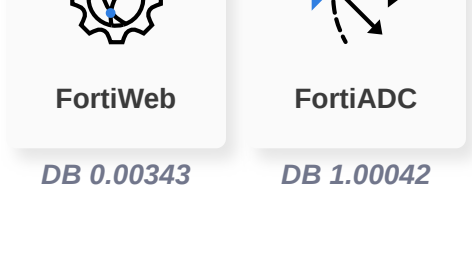
DB 22.503

DB 22.503

DB 22.503

#### Web App Security

Detects and blocks attack attempts related to CVE-2022-47986



DB 0.00343

DB 1.00042

### Installation

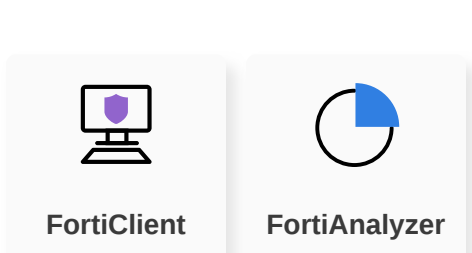
### C2

### Action

## DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

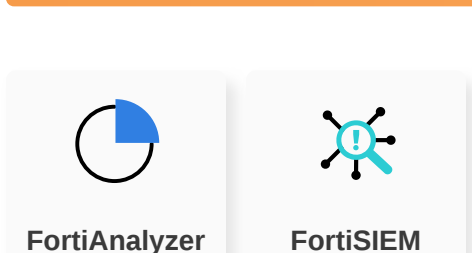
### Outbreak Detection



DB 1.7

DB 1.00090

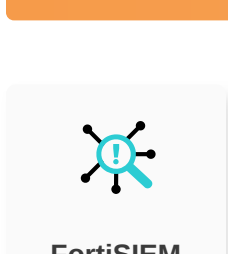
### Threat Hunting



v6.4+

v6.6+

### Content Update



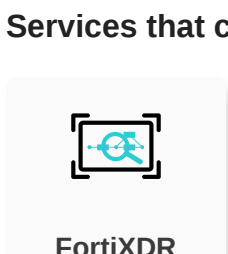
DB 313

## RESPOND

Develop containment techniques to mitigate impacts of security events:

### Automated Response

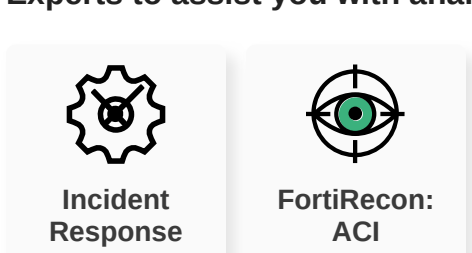
Services that can automatically respond to this outbreak.



FortiXDR

### Assisted Response Services

Experts to assist you with analysis, containment and response activities.



Incident Response

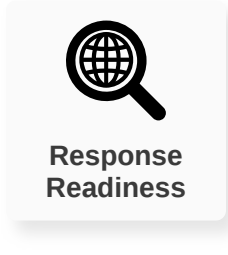
FortiRecon: ACI

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

### InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



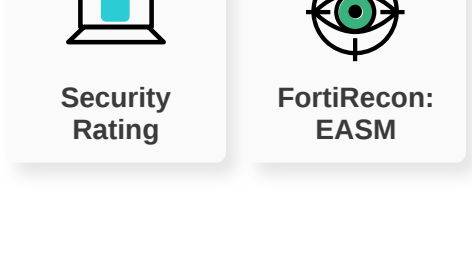
Response Readiness

## IDENTIFY

Identify processes and assets that need protection:

### Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



Security Rating

FortiRecon: EASM

## Additional Resources

**Security Week** <https://www.securityweek.com/recently-patched-ibm-aspera-faspex-vulnerability-exploited-in-the-wild/>

**The Record Media** <https://therecord.media/ibm-aspera-faspex-bug-cisa-known-vulnerability-list/>

**The Stack** <https://thetack.technology/ibm-aspera-faspex-exploited-cve-2022-47986/>

**The Hacker News** <https://thehackernews.com/2023/04/iranian-government-backed-hackers.html>

Learn more about [FortiGuard Outbreak Alerts](#)