

OUTBREAK ALERTS



Fortra GoAnywhere MFT RCE Vulnerability

Zero-day exploited in the wild

<https://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml#zerodayfe1>

CVEs: [CVE-2023-0669](#)

Fortra (formerly known as HelpSystems) GoAnywhere MFT contains a pre-authentication remote code execution vulnerability in the License Response Servlet.

Background

GoAnywhere MFT is a secure managed file transfer solution that streamlines the exchange of data between systems, employees, customers, and trading partners. The security flaw CVE-2023-0669, enables attackers to gain remote code execution on unpatched GoAnywhere MFT. According to the Fortra advisory, the exploit requires public internet access to the administrative console of the application.

Announced

February 1, 2023: Fortra posted a security advisory:

<https://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml#zerodayfe1>

February 7, 2023: Fortra released a patch (7.1.2) to address this actively exploited vulnerability.

Latest Developments

February 10, 2023: Clop ransomware claimed breaching about 130 organisations using GoAnywhere zero-day vulnerability to bleeping computer.

<https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/>

February 10, 2023: CISA added the CVE-2023-0669 GoAnywhere MFT vulnerability to its Known Exploited Vulnerabilities Catalog.

April 17, 2023: Summary of the Investigation related to CVE-2023-0669 posted by the vendor (Fortra).

<https://www.fortra.com/blog/summary-investigation-related-cve-2023-0669>

FortiGuard Labs recommends updating the vulnerable versions of GoAnywhere MFT and patch to version 7.1.2 as mentioned in the advisory as soon as possible and has released an IPS signature to detect and block any attack relating to the flaw CVE-2023-0669.

PROTECT

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

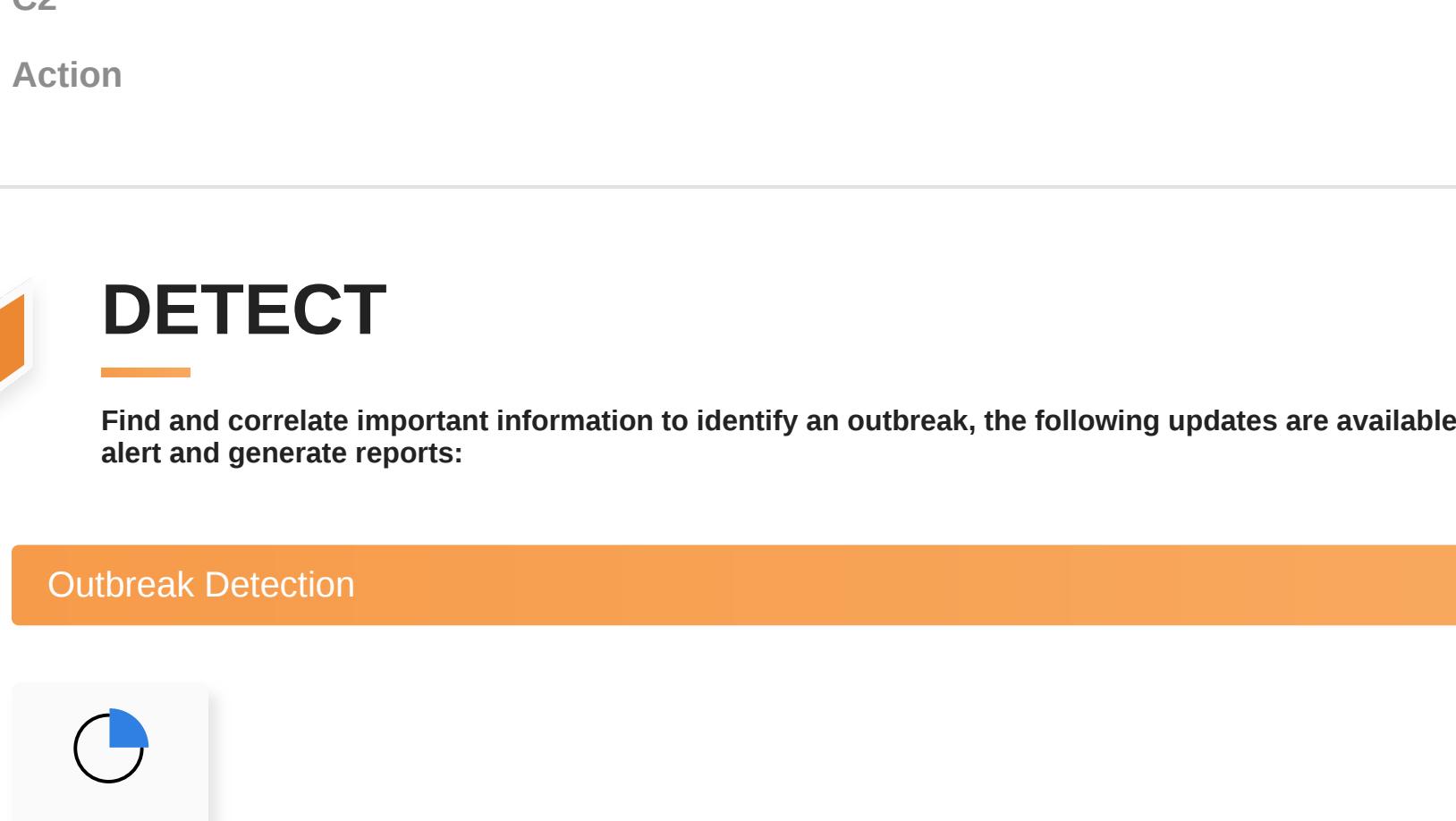
Reconnaissance

Weaponization

Delivery

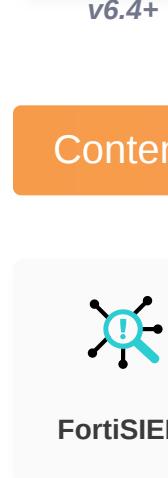
AV

Detects and blocks Clop Malware related to GoAnywhere MFT RCE (CVE-2023-0669)



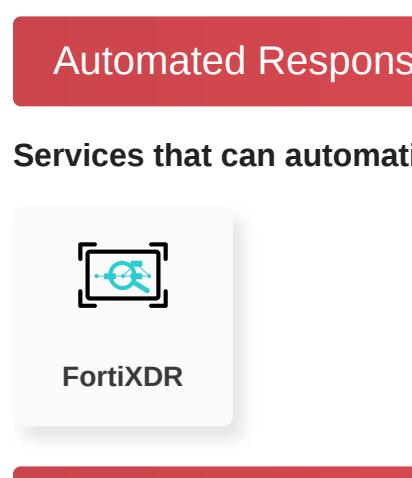
Vulnerability

Detects vulnerable GoAnywhere MFT (CVE-2023-0669)



AV (Pre-filter)

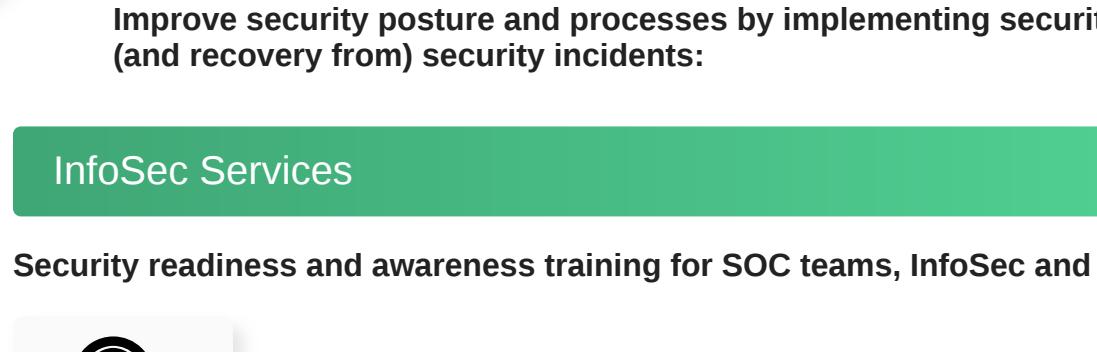
Detects and blocks Clop Malware related to GoAnywhere MFT RCE (CVE-2023-0669)



Exploitation

IPS

Detects and blocks attack attempts related to GoAnywhere MFT RCE (CVE-2023-0669)



Web App Security

Detects and blocks attack attempts related to GoAnywhere MFT RCE (CVE-2023-0669)

Installation

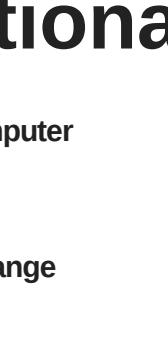
C2

Action

DETECT

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

Outbreak Detection



Threat Hunting



Content Update

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

Assisted Response Services

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

InfoSec Services

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

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.

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.

Additional Resources

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/>

InfoSec Exchange

<https://infosec.exchange/@briankrebs/109795710941843934>

Decipher

<https://duo.com/decipher/fortra-patches-actively-exploited-zero-day-in-goanywhere-mft>

Dark Reading

<https://www.darkreading.com/attacks-breaches/clop-keeps-racking-up-ransomware-victims-with-goanywhere-flaw>

Learn more about [FortiGuard Outbreak Alerts](#)

