FORTINET

OUTBREAK ALERTS

Fortra GoAnywhere MFT RCE Vulnerability

Zero-day exploited in the wild

https://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml#zerodayfeb1
CVEs: CVE-2023-0669

Fortra (formerly, knowns 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#zerodayfeb1

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 7.12 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)

FortiGate — DB 91.00582
FortiWeb — DB 91.00582
FortiClient — DB 91.00582
FortiSASE — DB 91.00582
FortiMail — DB 91.00582
FortiCASB — DB 91.00582
FortiCWP — DB 91.00582
FortiADC — DB 91.00582
FortiProxy — DB 91.00582

Vulnerability

Detects vulnerable GoAnywhere MFT (CVE-2023-0669)

FortiClient — DB 1.396

AV (Pre-filter)

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

FortiEDR — DB 91.00582
FortiNDR — DB 91.00582

- **Exploitation**

IPS

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

FortiGate — DB 22.495
FortiSASE — DB 22.495
FortiNDR — DB 22.495
FortiADC — DB 22.495
FortiProxy — DB 22.495

Web App Security

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

FortiWeb — DB 6.00348

- 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

FortiAnalyzer — DB 1.00087

Threat Hunting

FortiAnalyzer — v6.4+
FortiSIEM — v6.6+

Content Update

FortiSIEM — DB 404

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

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