



Microsoft Office and Windows HTML RCE Vulnerability

Unpatched Zero-day exploited in the wild

<https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/>

CVEs: CVE-2023-36884

Microsoft has identified a phishing campaign conducted by the threat actor tracked as Storm-0978 targeting defense and government entities in Europe and North America. The campaign involved the abuse of CVE-2023-36884, a remote code execution vulnerability exploited via specially crafted Microsoft Office documents spread using phishing techniques.

Background

Storm-0978 (also referred to as RomCom) is a cybercriminal group based out of Russia, known to conduct ransomware operations. Previously, Storm-0978 has been seen using the "Industrial Spy" ransomware and a ransomware variant called "Underground". Storm-0978 is also known to target organizations with trojanized versions of popular legitimate software. Some of the identified ransomware attacks have impacted the telecommunications, finance industries, and government institutions.

Announced

June 2023: According to the Microsoft blog, Storm-0978 conducted a phishing campaign containing a fake OneDrive loader to deliver a backdoor with similarities to RomCom. The phishing emails were directed to defense and government entities in Europe and North America. These emails led to exploitation via the CVE-2023-36884 vulnerability.

July 11, 2023: Microsoft released a detailed blog on the campaign targeting CVE-2023-36884.

<https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/>

Latest Developments

July 12, 2023: FortiGuard Labs has updated one of its IPS signature [MS.Office.RTF.File.OLE.autolink.Code.Execution] to detect and block file based triggers relating to exploitation of CVE-2023-36884 and AV updates to block known malware related to the campaign.

The IPS signature telemetry shows increased attack attempts over the last month and up to 4500+ unique IPS device detections in the month of June and July 2023.

FortiGuard Labs strongly suggests to follow Microsoft's Guide for mitigation and apply patches as soon as they become available to fully mitigate any risks.

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884>

July 17, 2023: CISA added CVE-2023-36884 to its Known Exploited Vulnerability catalog (KEV).

PROTECT

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

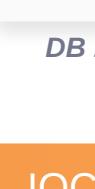
Reconnaissance

Weaponization

Delivery

AV

Detects and blocks known Malware leveraging Microsoft Office and Windows HTML RCE Vulnerability (CVE-2023-36884)



FortiGate

DB 9.05024



FortiWeb

DB 9.05024



FortiClient

DB 9.05024



FortiSASE

DB 9.05024



FortiMail

DB 9.05024



FortiCASB

DB 9.05024



FortiCWP

DB 9.05024

FortiADC

FortiProxy

DB 9.05024

DB 9.05024

Vulnerability

Detects vulnerable instances of Microsoft Office (CVE-2023-36884)



FortiClient

v5.0+

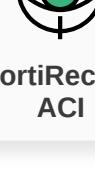
AV (Pre-filter)

Detects and blocks known Malware leveraging Microsoft Office and Windows HTML RCE Vulnerability (CVE-2023-36884)



FortiEDR

DB 9.05024



FortiSandbox

DB 9.05024



FortiNDR

DB 9.05024



FortiADC

DB 9.05024



FortiProxy

DB 9.05024

Exploitation

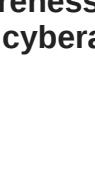
IPS

Detects and blocks attacks leveraging Microsoft Office and Windows HTML RCE Vulnerability (CVE-2023-36884)



FortiGate

DB 21.336



FortiSASE

DB 21.336



FortiNDR

DB 21.336



FortiADC

DB 21.336



FortiProxy

DB 21.336

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



FortiClient

DB 1.12



FortiAnalyzer

DB 2.00012

IOC



FortiAnalyzer

v6.4+



FortiSIEM

v6.6+



FortiSOCaaS

Threat Hunting

FortiAnalyzer

v6.4+

FortiSIEM

v6.6+

Content Update

FortiSIEM

DB 3.10

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak:

FortiKDR

DB 9.05024

Assisted Response Services

FortiIncident

DB 9.05024

FortiACI

DB 9.05024

Incident Response

C2

Action

RECOVER

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

NOC/SOC Training

undefined

NSE Training

DB 9.05024

Response Readiness

DB 9.05024

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness

DB 9.05024

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security

Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon

EASM

Additional Resources

Bleeping Computer

<https://www.bleepingcomputer.com/news/security/microsoft-unpatched-office-zero-day-exploited-in-nato-summit-attacks/>

Security Week

<https://www.securityweek.com/microsoft-warns-of-office-zero-day-attacks-no-patch-available/>