EnCyb

Severity: Critical

Advisory Type: Threat

APT28 Exploiting Microsoft Office RTF Zero-Day

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Researchers have linked a likely APT28-associated threat actor to the exploitation of a Microsoft Office RTF zero-day (CVE-2026-21509) to deliver modular malware in a multi-stage campaign targeting Central and Eastern Europe.

- CVE: CVE-2026-21509
- CVSS: 9.8
- Affected Sector: Government, Defence, Diplomatic, and Related Organizations
- Affected Product: Microsoft Office (RTF handling)
- Affected Region: Central & Eastern Europe
- Severity: Critical
- Published Date: February 02, 2026

TECHNICAL DETAILS

- **Target:** End users within targeted organizations using Microsoft Office, particularly staff handling document-based communications such as emails, reports, contracts, or official correspondence. These users often have regular exposure to external documents, increasing their attack surface.

- **Root Cause:** A zero-day remote code execution vulnerability in Microsoft Office's RTF file handling (CVE-2026-21509) that allows attackers to execute arbitrary code when a malicious RTF file is processed.

- **Prerequisite For Exploitation:** User interaction is required—specifically, opening a specially crafted malicious RTF document in Microsoft Office. No additional privileges are needed, making exploitation highly effective in phishing-based delivery scenarios.

INDICATORS OF COMPROMISE

TYPE	VALUES
File Hash (MD5)	95e59536455a089ced64f5af2539a449
File Hash (SHA1)	4592e6173a643699dc526778aa0a30330d16fe08
File Hash (SHA256)	b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546
File Hash (MD5)	2f7b4dca1c79e525aef8da537294a6c4
File Hash (SHA1)	c4799d17a4343bd353e0edb0a4de248b99295d4d
File Hash (SHA256)	1ed863a32372160b3a25549aad25d48d5352d9b4f58d4339408c4eea69807f50
File Hash (MD5)	4727582023cd8071a6f388ea3ba2feaa
File Hash (SHA1)	d788d85335e20bb1f173d4d0494629d36083dddc
File Hash (SHA256)	5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02
File Hash (MD5)	d47261e52335b516a777da368208ee91
File Hash (SHA1)	c8c84bf33c05fb3a69bc5e2d6377b73649b93dce
File Hash (SHA256)	fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b
File Hash (MD5)	7c396677848776f9824ebe408bbba943
File Hash (SHA1)	d577c4a264fee27084ddf717441eb89f714972a5
File Hash (SHA256)	c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f
File Hash (MD5)	f3b869a8d5ad243e35963ba6d7f89855
File Hash (SHA1)	c1b272067491258ea4a2b1d2789d82d157aaf90a
File Hash (SHA256)	a944a09783023a2c6c62d3601cbd5392a03d808a6a51728e07a3270861c2a8ee
File Hash (MD5)	f05d0b13c633ad889334781cf4091d3e
File Hash (SHA1)	7bbb530eb77c6416f02813cd2764e49bd084465c
File Hash (SHA256)	bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e
File Hash (MD5)	859c4b85ed85e6cc4eadb1a037a61e16
File Hash (SHA1)	da1c3e92f69e6ca0e4f4823525905cb6969a44ad
File Hash (SHA256)	0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e
File Hash (MD5)	e4a5c4b205e1b80dc20d9a2fb4126d06
File Hash (SHA1)	e52a9f004f4359ea0f8f9c6eb91731ed78e5c4d3
File Hash (SHA256)	a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1
File Hash (MD5)	154ff6774294e0e6a46581c8452a77de
File Hash (SHA1)	22da6a104149cad87d5ec5da4c3153bebf68c411
File Hash (SHA256)	2822c72a59b58c00fc088aa551cdeeb92ca10fd23e23745610ff207f53118db9
File Hash (MD5)	ee0b44346db028a621d1dec99f429823
File Hash (SHA1)	cea7e9323d79054f92634f4032c26d30c1cedd7e
File Hash (SHA256)	9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8

File Hash (MD5)	ea6615942f2c23dba7810a6f7d69e2da
File Hash (SHA1)	23b6f9c00b9d5475212173ec3cbbcff34c4400a7
File Hash (SHA256)	3f446d316efe2514efd70c975d0c87e12357db9fca54a25834d60b28192c6a69
Domain	freefoodaid[.]com
Domain	wellnesscaremed[.]com
URL	hxxps://freefoodaid[.]com/documents/2_2.d
URL	hxxps://freefoodaid[.]com/tables/tables.d
URL	hxxps://freefoodaid[.]com/documents/2_2.lNk

IMPACT

- Remote code execution on victim systems
- Unauthorized access to emails and sensitive data
- Persistent attacker presence within the environment
- Potential lateral movement and further compromise
- Risk of regulatory, operational, and reputational impact

RECOMMENDATIONS

- Immediately apply Microsoft security updates addressing CVE-2026-21509
- Block and monitor known IOCs associated with the vulnerability across security controls
- Block or restrict RTF file handling where not required
- Disable or tightly control Office and Outlook macros
- Inspect systems for suspicious DLLs, VBA projects, and scheduled tasks
- Enhance email security to detect and quarantine malicious attachments

REFERENCE

- https://gbhackers.com/microsoft-office-zero-day/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com