It's Probably Nothing
by Sierra Echo Charlie

EDITION 03 / 15 OCTOBER 2026

Record Patch Tuesday, a phishing takedown, and laptop farms

An exploited Mark-of-the-Web bypass, 1bn+ scam messages' worth of domains seized, and Texas raids.

4 stories / Listen online - 4:36

THE TAKEAWAY

A bit calmer than the last couple of days. Microsoft shipped a record-sized Patch Tuesday with one exploited bug that matters to almost everyone. There's also a takedown aimed at the phishing kits behind those parcel and toll texts, and some US raids on North Korean laptop farms.

01 / THE BRIEF

Microsoft's biggest Patch Tuesday yet includes an exploited Mark-of-the-Web bypass

The count depends on who did the maths. BleepingComputer has 1,411 flaws, 70 of them Critical, and SecurityWeek's headline says 1,413. Either way, it's a record, and the one that matters is CVE-2026-96951. Microsoft describes it as a command injection flaw in Windows Shell that lets an unauthorised attacker bypass a security feature over a network. Reporting says the feature is Mark of the Web, which is the thing that triggers SmartScreen and Protected View warnings on files that came from somewhere sketchy. Microsoft says it's exploited, though it needs a user to act on a crafted file, such as one sent by email or IM. It hasn't shared anything about the attacks. CISA added it to KEV on 13 October and gave federal agencies until 16 October. According to SecurityWeek, researchers at Fujitsu and Anthropic, plus an independent researcher, each reported it separately, which suggests it wasn't exactly well hidden.

The two publicly disclosed bugs are less urgent. CVE-2026-108398 is a .NET Framework WDAC bypass found by James Forshaw, and Microsoft rates exploitation unlikely. CVE-2026-92707 is a MessagePack-CSharp denial-of-service bug. Mallory's summary also flags CVE-2026-103572 (CVSS 8.8), an RCE via indirect prompt injection in the Copilot component shared by Visual Studio and SSMS. We haven't checked that one against Microsoft's advisory.

A MotW bypass isn't a crisis on its own, but it removes one of the few speed bumps between a phishing attachment and execution. That makes it a good fit for this week's other story.

WORTH ASKING

This is the last update for Windows 11 24H2 Home and Pro and Windows 10 Enterprise LTSB 2016, so if any of those are hanging around, they've just become a different kind of problem.

QUALIFICATIONS

We couldn't read Microsoft's advisory directly, so the details come from trade reporting and the KEV feed.

SOURCES

Microsoft Patches Exploited Windows Shell Flaw and Copilot Remote Code Execution (Mallory) - Reporting / context

Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days - Reporting / context

Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day - Reporting / context

CISA Known Exploited Vulnerabilities catalogue (JSON feed) - Primary source

02 / THE BRIEF

Microsoft seizes domains behind three Chinese-language phishing services

Microsoft, working with Japan's National Police Agency and Health-ISAC, got a US court order to seize and redirect domains behind YAM Store, CoGUI and Iron Man. Health-ISAC, relaying Microsoft's figures, says that since January the three have enabled more than a billion malicious messages aimed at more than 75,000 organisations in more than 150 countries. The Record reports that Microsoft also disabled more than 20,000 YAM Store-linked accounts and is blocking more than 100,000 impersonation domains. It says Iron Man sells thousands of templates tailored to Australia, Japan, India and others: postal services, traffic fines, tax agencies, banks and telcos. In other words, the stuff in your family group chat. Proofpoint says the CoGUI-family campaigns mostly hit Japan, with some landing in the US, Australia and Italy.

Proofpoint expects this to dent the kits' effectiveness. Mallory notes nobody has shown a lasting drop in volume yet, and PhaaS operators do tend to have spare domains lying about.

SOURCES

Microsoft and Partners Disrupt Phishing Ecosystem Behind More Than 1 Billion Messages (Mallory) - Reporting / context

Disrupting the service economy behind transnational cybercrime operations (Health-ISAC) - Primary source

Disruption targets major Chinese-language phishing kits with Japanese focus (Proofpoint) - Primary source

Microsoft takes down 3 major phishing platforms used by Chinese cybercriminals - Reporting / context

03 / THE BRIEF

US raids Texas laptop farms in North Korean IT-worker crackdown

The DOJ's Operation Lonestar Roundup searched suspected laptop farms in Texas and seized about 187 devices. SecurityWeek says investigators searched 40 locations. An Ohio indictment charges US nationals Michael James Bostelle and Juan Cecilio Pena Carrillo, who were arrested, along with ten China-based defendants. All of them are presumed innocent. DOJ says the scheme hit more than 70 US employers and brought in about US$3 million for DPRK-controlled entities. Per Mallory's summary, CrowdStrike linked the activity to Famous Chollima and expects only limited, local disruption. That sounds about right for a model that just needs another spare bedroom full of laptops.

QUALIFICATIONS

The CrowdStrike attribution comes via Mallory's summary and wasn't checked against CrowdStrike's own material.

SOURCES

DOJ Arrests Two in North Korean Laptop-Farm Scheme Targeting U.S. Employers (Mallory) - Reporting / context

Justice Department Announces Coordinated Actions to Combat North Korean Remote IT Worker Schemes Affecting More than 70 U.S. Companies - Primary source

US Arrests Two in Crackdown on North Korean IT Worker Laptop Farms - Reporting / context

04 / THE BRIEF

French fridge attack count reportedly reaches about 700 stores

A short update on the supermarket refrigeration story. ComplexDiscovery, citing AP, reports that Finance Minister Roland Lescure told Parliament on Tuesday that about 700 of France's roughly 10,000 supermarkets were affected, and that food supply wasn't at risk. That's about double the earlier tallies. The same report says Copeland acknowledged a 'vulnerability' in a discontinued, end-of-life generation of controllers, though it hasn't confirmed any compromises in France. It also says a Reuters scan found at least 4,500 Danfoss web interfaces still online.

QUALIFICATIONS

All of this comes through one aggregator relaying AP. AP doesn't say how the 700 figure was compiled, and the remarks may predate today's window. Nothing links the attack to a specific Copeland or Danfoss CVE.

SOURCES

Cyberattack Manipulates Refrigeration at French Supermarkets, Destroying Fresh Stock (Mallory) - Reporting / context

Refrigeration hack affected about 700 French supermarkets, government says, as Danfoss interfaces stay online - Reporting / context

Incident de sécurité ciblant les contrôleurs à distance des installations de réfrigération - CERT-FR (CERTFR-2026-ALE-012) - Primary source

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.