## Week of January 13, 2025

# Cybersecurity Headlines

## Official Security Bulletins

*Headlines from List of Official Government Sources*

### Securing Federal Networks: Evolving to an Enterprise Approach

www.cisa.gov

In December 2020, organizations across the world were notified that they were victims of a Russian cyberattack. The Russians had compromised the widely used SolarWinds Orion software platform and infected thousands of clients with a corrupted update.

NSA joins CISA and others in releasing:

SECURE BY DEMAND:
PRIORITY CONSIDERATIONS FOR OPERATIONAL TECHNOLOGY OWNERS AND OPERATORS IN THE SELECTION OF DIGITAL PRODUCTS

CYBERSECURITY INFORMATION SHEET

### NSA and Others Publish Guidance for Secure OT Product Selection

www.nsa.gov

FORT MEADE, Md. - The National Security Agency (NSA) joins the Cybersecurity and Infrastructure Security Agency (CISA) and other organizations to publish guidance helping operational technology (OT) owners and operators integrate security when select...

### CISA Publishes Microsoft Expanded Cloud Log Implementation Playbook

www.cisa.gov

Guides organizations with using new logging capabilities to detect and defend against sophisticated cyber threat actors. WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA), in close coordination with the Office of Management and...

### Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the co...

### Critical Patches Issued for Microsoft Products, January 14, 2025

www.cisecurity.org

Multiple vulnerabilities have been discovered in Microsoft products, the most severe of which could allow for remote code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then ...

### Multiple Vulnerabilities in Fortinet Products Could Allow for Remote Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered Fortinet Products, the most severe of which could allow for remote code execution. FortiManager is a network and security management tool that provides centralized management of Fortinet devices from a si...

### Multiple Vulnerabilities in Ivanti Avalanche Could Allow for Authentication Bypass

www.cisecurity.org

Multiple Vulnerabilities have been discovered in Ivanti Avalanche, the most severe of which could allow for authentication bypass. Details of these vulnerabilities are as follows: Tactic: Initial Access ():. Technique: Exploit Public-Facing Applicati...

NSA and others are releasing:

CLOSING THE SOFTWARE UNDERSTANDING GAP

CYBERSECURITY INFORMATION SHEET

### NSA Jointly Releases Recommendations for Closing the Software Understanding Gap > National Security Agency/Central Security Service > Press Release View

www.nsa.gov

FORT MEADE, Md. – A report released by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), the Defense Advanced Research Projects Agency (DARPA), and the Office of the Under Secretary of Defense for Research and En...

### Office of Public Affairs | Justice Department and FBI Conduct International Operation to Delete Malware Used by China-Backed Hackers - United States Department of Justice

www.justice.gov

The Justice Department and FBI today announced a multi-month law enforcement operation that, alongside international partners, deleted "PlugX" malware from thousands of infected computers worldwide. As described in court documents unsealed in the Eas...

## Cybercrimes, Scams & Incidents

*Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks*

### Chinese Innovations Spawn Wave of Toll Phishing Via SMS

krebsonsecurity.com

In each case, the emergence of these SMS phishing attacks coincided with the release of new phishing kit capabilities that closely mimic these toll operator websites as they appear on mobile devices.

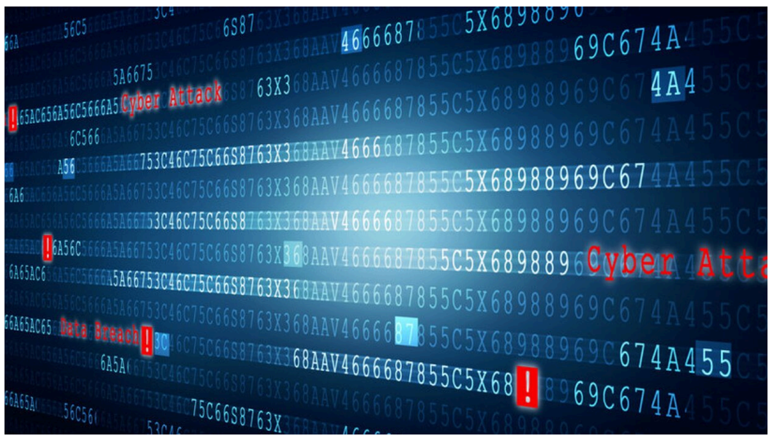
### Microsoft MFA outage blocking access to Microsoft 365 apps

www.bleepingcomputer.com

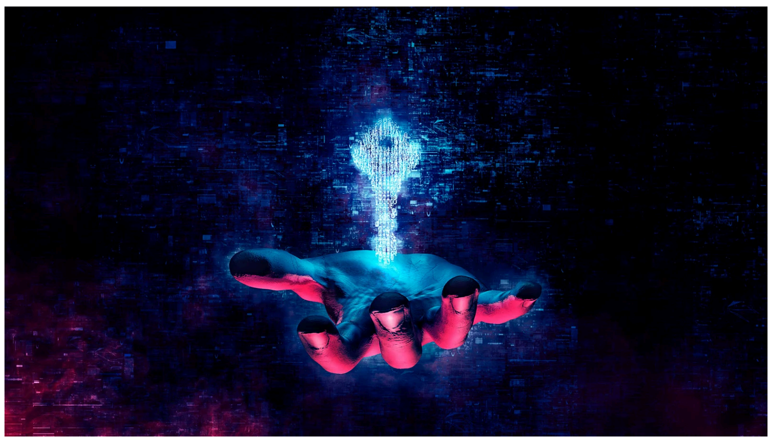
Microsoft is investigating an ongoing Multi-Factor Authentication (MFA) outage that is blocking customers from accessing Microsoft 365 Office apps.

Some affected Microsoft 365 users have also reported that MFA registration and reset are not working.

"Users may be unable to access some Microsoft 365 Apps when authenticating with MFA," Microsoft said in an incident alert published in the admin cen



www.govtech.com



### Ransomware abuses Amazon AWS feature to encrypt S3 buckets - BleepingComputer

www.bleepingcomputer.com

A new ransomware campaign encrypts Amazon S3 buckets using AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) known only to the threat actor, demanding ransoms to receive the ...

## Industry News

*Headlines collected from across the cybersecurity industry related to legislation, business, and big tech*

### Redefining third-party governance and identity for the cloud-first era

www.scworld.com

The rapid evolution of digital ecosystems, driven by cloud-first technologies and software-as-a-service (SaaS) models, has exposed glaring weaknesses in traditional third-party governance practices.

### Microsoft Takes Legal Action Against AI "Hacking as a Service" Scheme - Schneier on Security

www.schneier.com

Microsoft Takes Legal Action Against AI "Hacking as a Service" Scheme. Not sure this will matter in the end, but it's a positive move:. Microsoft is accusing three individuals of running a "hacking-as-a-service" scheme that was designed to allow the ...

### Biden administration rolls out wide-reaching cybersecurity executive order

www.cybersecuritydive.com

The order follows a rash of state-linked campaigns, including the hack of nine telecom companies by Salt Typhoon as well as a separate attack against the Treasury Department connected to the compromise of BeyondTrust customers. The recent attacks hav...

### From AI to FedRAMP: 5 agency takeaways from Biden's cyber executive order | FedScoop

fedscoop.com

The Biden White House's last-minute flurry of tech policy activity continued Thursday with the release of the president's long-awaited executive order on cybersecurity, a bookend to his 2021 EO that dictates agency action on everything from securing ...

### Hack of Rhode Island social services platform impacted at least 709K, officials say - Cybersecurity Dive

www.cybersecuritydive.com

Rhode Island began mailing notification letters Friday to alert individuals impacted by the December ransomware attack against the state social services agency, Gov. Dan McKee said during a Friday press conference.. Officials estimate the information...

### OPM awards $149M cyber, network operations support contract

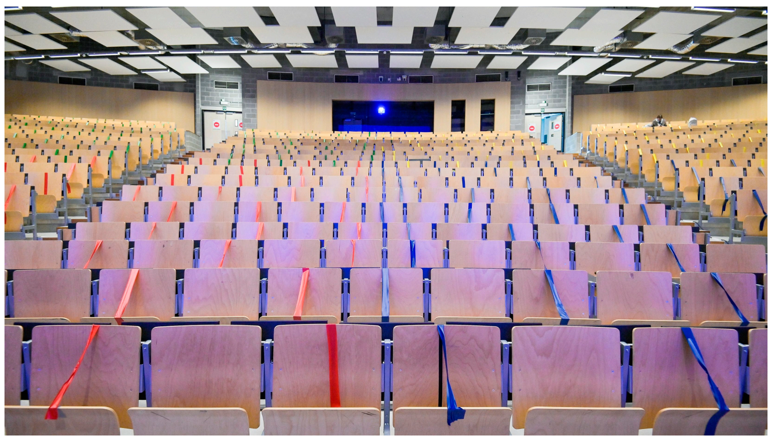
www.govexec.com

Bering Straits Professional Services has won a potential five-year, $149 million contract for broad cybersecurity infrastructure and network operations support services to the federal government ...

### Phishing click rates tripled in 2024 despite user training

www.csoonline.com

For years organizations have invested in security awareness training programs to teach employees how to spot and report phishing attempts. Despite those efforts, enterprise users were three times ...



### What is 'security theater' and how can we move beyond it?

cyberscoop.com

Alert fatigue and shadow access are just two examples of "security theater." The broader problem is that most organizations are being swept up in security theatrics instead of adopting meaningful security measures.

### Microsoft: Happy 2025. Here's 161 Security Updates

krebsonsecurity.com

Microsoft today unleashed updates to plug a whopping 161 security vulnerabilities in Windows and related software, including three "zero-day" weaknesses that are already under active attack.

***Please be advised that** the following resources and materials are for informational purposes only. **The opinions and views expressed in these materials** are the opinions of the designated authors and do not reflect the opinions or views of **the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth).** The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.*

## Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA
- White house | ONCD

## External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record