Massive Microsoft 365 outage caused by WAN router IP change

By
**Sergiu Gatlan
(https://www.bleepingcomputer.com
/author/sergiu-gatlan/)**

January 27, 2023   03:32 PM   **0**

Microsoft says this week's five-hour-long Microsoft 365 worldwide outage
was caused by a router IP address change that led to packet forwarding
issues between all other routers in its Wide Area Network (WAN).

Redmond said at the time (https://www.bleepingcomputer.com
/news/microsoft/microsoft-365-outage-takes-down-teams-exchange-

online-outlook/) that the outage resulted from DNS and WAN networking configuration issues caused by a WAN update and that users across all regions serviced by the impacted infrastructure were having problems accessing the affected Microsoft 365 services.

The issue led to service impact in waves, peaking approximately every 30 minutes as shared on the Microsoft Azure service status page (this status page was also affected as it intermittently displayed "504 Gateway Time-out" errors).

Top Stories

(https://www.bleepingcomputer.com/news/security/google-ads-push-virtualized-malware-made-for-antivirus-evasion-/?traffic_source=Connatix)

Google ads push 'virtualized' malware made for antivirus evasion

The list of services impacted by the outage included Microsoft Teams, Exchange Online, Outlook, SharePoint Online, OneDrive for Business, PowerBi, Microsoft 365 Admin Center, Microsoft Graph, Microsoft Intune, Microsoft Defender for Cloud Apps, and Microsoft Defender for Identity,

In all, it took Redmond over five hours to address the issue, from 7:05 AM UTC when it started investigating up until 12:43 PM UTC when service was restored.

"Between 07:05 UTC and 12:43 UTC on 25 January 2023, customers experienced issues with networking connectivity, manifesting as long network latency and/or timeouts when attempting to connect to resources hosted in Azure regions, as well as other Microsoft services including Microsoft 365 and Power Platform," Microsoft said (https://status.azure.com/en-us/status/history /#:~:text=Preliminary%20Post%20Incident%20Review%20(PIR) %20%E2%80%93%20Azure%20Networking%20%E2%80%93 %20Global%20WAN%20issues%20(Tracking%20ID%20VSG1%2DB90)) in a preliminary post-incident report published today.

"While most regions and services had recovered by 09:00 UTC, intermittent packet loss issues were fully mitigated by 12:43 UTC. This incident also impacted Azure Government cloud services that were dependent on Azure public cloud."

> *We've confirmed that the impacted services have recovered and remain stable. We're investigating some potential impact to the Exchange Online Service. Further, updates on the Exchange investigation will be available in your admin center under the SI# EX502694.*
>
> *— Microsoft 365 Status (@MSFT365Status) January 25, 2023 (https://twitter.com/MSFT365Status/status /1618255289165168640?ref_src=twsrc%5Etfw)*

Microsoft now also revealed that the issue was triggered when changing the IP address of a WAN router using a command that had not been thoroughly vetted and that has different behaviors on different network devices.

"As part of a planned change to update the IP address on a WAN router, a command given to the router caused it to send messages to all other routers in the WAN, which resulted in all of them recomputing their adjacency and forwarding tables," Microsoft said.

"During this re-computation process, the routers were unable to correctly forward packets traversing them."

While the network began recovering on its own starting at 08:10 UTC, the automated systems responsible for maintaining the health of the wide area network (WAN) paused due to the impact on the network.

These systems included those for identifying and eliminating unhealthy devices as well as traffic engineering systems for optimizing data flow across the network.

As a result of the pause, some network paths continued experiencing increased packet loss from 9:35 UTC until the systems were manually restarted, returning the WAN to optimal operating conditions and completing the recovery process at 12:43 UTC.

Following this incident, Microsoft says that it's now blocking highly impactful commands from being executed and that it will also require all command execution to follow guidelines for safe configuration changes.

Related Articles:

Microsoft 365 outage takes down Teams, Exchange Online, Outlook
(https://www.bleepingcomputer.com/news/microsoft/microsoft-365-
outage-takes-down-teams-exchange-online-outlook/)

Microsoft disables verified partner accounts used for OAuth phishing
(https://www.bleepingcomputer.com/news/security/microsoft-disables-
verified-partner-accounts-used-for-oauth-phishing/)

Attackers can hide 'external sender' email warnings with HTML and CSS
(https://www.bleepingcomputer.com/news/security/attackers-can-hide-
external-sender-email-warnings-with-html-and-css/)

Microsoft 365 trial offer blocks access to Windows 10 desktops
(https://www.bleepingcomputer.com/news/microsoft/microsoft-365-
trial-offer-blocks-access-to-windows-10-desktops/)

Become proficient in Microsoft Excel from home with this deal
(https://www.bleepingcomputer.com/offer/deals/become-proficient-in-
microsoft-excel-from-home-with-this-deal/)

AZURE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/AZURE/)

EXCHANGE ONLINE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EXCHANGE-ONLINE/)

MICROSOFT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT/)

MICROSOFT 365 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT-365/)

MICROSOFT TEAMS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MICROSOFT-TEAMS/)

OUTAGE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/OUTAGE/)

OUTLOOK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/OUTLOOK/)

(https://www.bleepingcomputer.com
/author/sergiu-
gatlan/)

SERGIU GATLAN (HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR /SERGIU-GATLAN/)
✉ (MAILTO:SERGIU@BLEEPINGCOMPUTER.COM) 🐦 (HTTPS://TWITTER.COM/SERGHEI)

Sergiu Gatlan has covered cybersecurity, technology, and a few other topics for over a decade. Email or Twitter DMs for tips.

‹ PREVIOUS ARTICLE	NEXT ARTICLE ›
(HTTPS://WWW.BLEEPINGCOMPUTER.COM	(HTTPS://WWW.BLEEPINGCOMPUTER.COM
/NEWS/SECURITY/UKRAINE-	/NEWS/SECURITY/THE-WEEK-
SANDWORM-HACKERS-HIT-	IN-RANSOMWARE-JANUARY-
NEWS-AGENCY-WITH-5-DATA-	27TH-2023-WE-HACKED-THE-
WIPERS/)	HACKERS/)

Post a Comment

Community Rules (https://www.bleepingcomputer.com/posting-guidelines/)

You need to login in order to post a comment

Login

Not a member yet? Register Now (https://www.bleepingcomputer.com/forums /index.php?app=core&module=global&section=register)

You may also like:

POPULAR STORIES

New Nevada Ransomware targets Windows and VMware ESXi systems

(https://www.bleepingcomputer.com
/news/security/new-nevada-
ransomware-targets-windows-
and-vmware-esxi-systems/)

Google Fi data breach let hackers carry out SIM swap attacks

(https://www.bleepingcomputer.com
/news/security/google-fi-data-
breach-let-hackers-carry-out-sim-
swap-attacks/)

FOLLOW US:

(https://www.facebook.com/BleepingComputer) (https://twitter.com/BleepinComputer) (https://mastodon.social/@bleepingcomputer) (https://www.youtube.com/user/BleepingComputer) (https://www.bleepingcomputer.com/feed/)

MAIN SECTIONS

News (https://www.bleepingcomputer.com/)

Downloads (https://www.bleepingcomputer.com/download/)

Virus Removal Guides (https://www.bleepingcomputer.com/virus-removal/)

Tutorials (https://www.bleepingcomputer.com/tutorials/)

Startup Database (https://www.bleepingcomputer.com/startups/)

Uninstall Database (https://www.bleepingcomputer.com/uninstall/)

Glossary (https://www.bleepingcomputer.com/glossary/)

COMMUNITY

Forums (https://www.bleepingcomputer.com/forums/)

Forum Rules (https://www.bleepingcomputer.com/forum-rules/)

Chat (https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/)

USEFUL RESOURCES

Welcome Guide (https://www.bleepingcomputer.com/welcome-guide/)

Sitemap (https://www.bleepingcomputer.com/sitemap/)

COMPANY

About BleepingComputer (https://www.bleepingcomputer.com/about/)

Contact Us (https://www.bleepingcomputer.com/contact/)

Send us a Tip! (https://www.bleepingcomputer.com/news-tip/)

Advertising (https://www.bleepingcomputer.com/advertise/)

Write for BleepingComputer (https://www.bleepingcomputer.com/write-for-bleepingcomputer/)

Social & Feeds (https://www.bleepingcomputer.com/rss-feeds/)

Changelog (https://www.bleepingcomputer.com/changelog/)

Terms of Use (https://www.bleepingcomputer.com/terms-of-use/) - Privacy Policy (https://www.bleepingcomputer.com/privacy/) - Ethics Statement (https://www.bleepingcomputer.com/ethics-statement/)