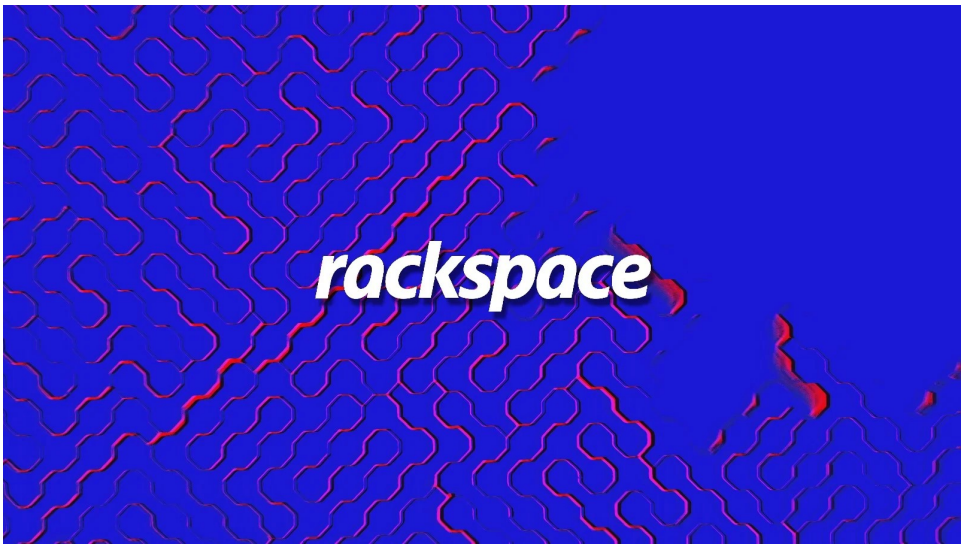
Rackspace: Ongoing Exchange outage caused by security incident

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

December 2, 2022 04:15 PM 2

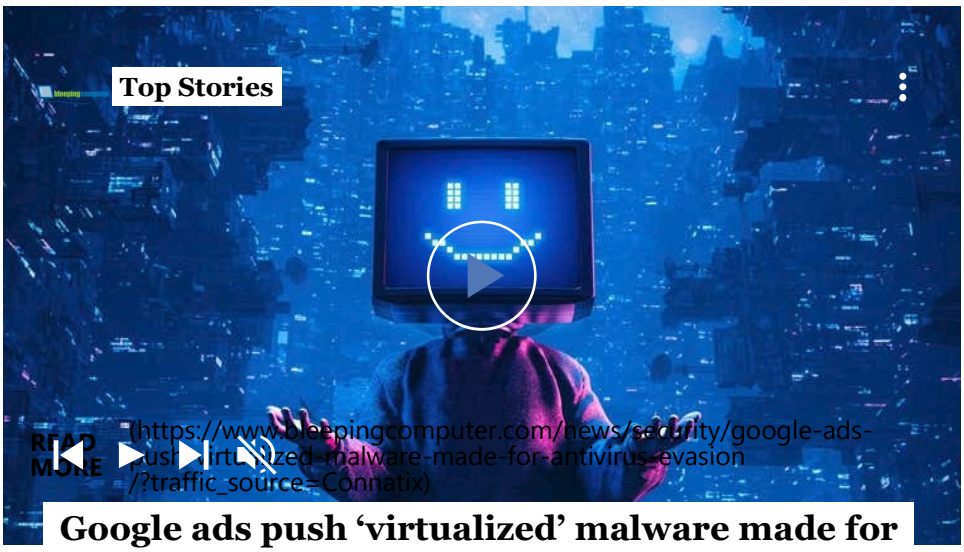


American cloud computing services provider Rackspace says an ongoing outage affecting its hosted Microsoft Exchange environments and likely thousands of customers was caused by a security incident.

The list of impacted services includes MAPI/RPC, POP, IMAP, SMTP, ActiveSync, and the Outlook Web Access (OWA) interface used to access

the Hosted Exchange instance to manage email online.

"We are investigating an issue that is affecting our Hosted Exchange environments. More details will be posted as they become available," Rackspace said on Friday night, at 02:49 AM EST, when it acknowledged the outage.



More than 15 hours later and multiple updates without any info on what is causing what it describes as a "system disruption," the company said it's "aware of an issue impacting" Hosted Exchange environments and that its engineering teams continue to work "to come to a resolution."

Affected customers were advised (https://twitter.com/Rackspace/status/1598800773047099403) to check the status page for the latest updates, even though those are also lacking details about the outage's root cause.

In reply, Rackspace's irked customers asked the company on social media (https://twitter.com/Rackspace/status/1598761923008266240) to provide an ETA for when the issue behind this outage will be addressed and shared plans to switch to another, more transparent, managed service provider (MSP).

Products	Status	Time
Hosted Exchange	System disruption [details]	1:54 PM EST
MAPI/RPC	System disruption	1:54 PM EST
POP	System disruption	1:54 PM EST
IMAP	System disruption	1:54 PM EST
SMTP	System disruption	1:54 PM EST
Outlook Web Access	System disruption	1:54 PM EST
ActiveSync	System disruption	1:54 PM EST

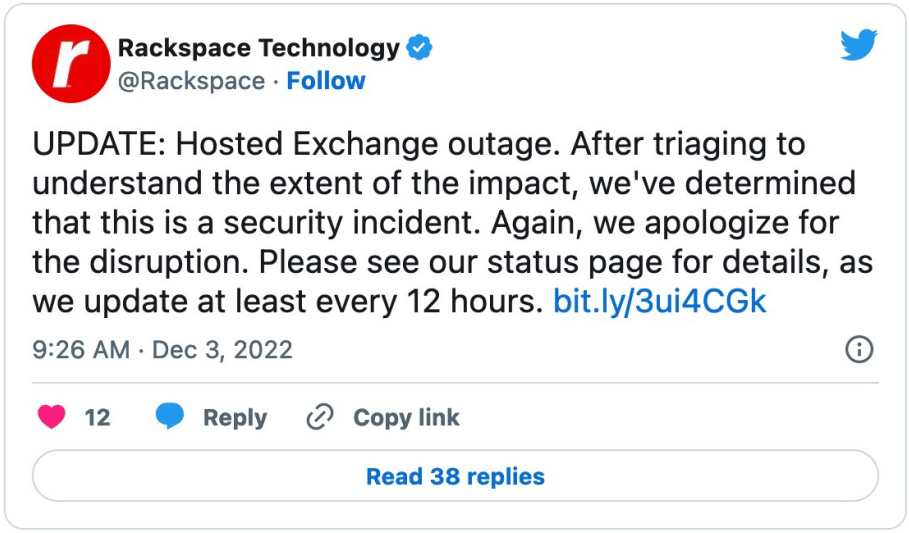
Rackspace Exchange outage

Almost twenty-four hours later, at 01:57 AM EST, Rackspace revealed the true cause of the outage, a security incident "isolated to a portion of our Hosted Exchange platform" that forced the company to disconnect the Hosted Exchange environment.

"On Friday, Dec 2, 2022, we became aware of an issue impacting our Hosted Exchange environment. We proactively powered down and disconnected the Hosted Exchange environment while we triaged to understand the extent and the severity of the impact," the company said (http://twitter.com/Rackspace/status/1598941743063322625).

"After further analysis, we have determined that this is a security incident. The known impact is isolated to a portion of our Hosted Exchange platform."

This confirms some of its customers' concerns who, due to the limited information, said that they feared the outage might be the result of a malware or ransomware attack.



(https://twitter.com/Rackspace/status/1598941743063322625)

Rackspace's Head of Global Public Relations Natalie Silva told BleepingComputer in an email sent Friday evening that the MSP is now providing affected customers with Microsoft Exchange Plan 1 licenses and instructions on how to migrate their email to Microsoft 365 until the outage is addressed.

"As we continue to work through the root cause of the issue, we

have provided an alternate solution that will re-activate our customers' ability to send and receive emails by providing access to an alternative email solution at no cost to them," Silva said.

"This solution will allow our impacted customers to resume regular business as soon as possible."

Detailed instructions on how to activate the free licenses and how to migrate users' mailboxes to Microsoft 365 are available in Rackspace's incident report (https://status.apps.rackspace.com/index/viewincidents?group=2).

The ProxyNotShell vulnerability

While Rackspace has shared very little information about the attack, cybersecurity expert Kevin Beaumont (https://cyberplace.social/@GossiTheDog) has shared a possible explanation.

Beaumont told BleepingComputer that Rackspace appears to have been running a Microsoft Exchange server vulnerable to the ProxyNotShell vulnerability.

ProxyNotShell was a zero-day vulnerability discovered to be actively exploited (https://www.bleepingcomputer.com/news/security/new-microsoft-exchange-zero-days-actively-exploited-in-attacks/) in September 2022 to install web shells on Microsoft Exchange servers.

Microsoft fixed the vulnerability (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-proxynotshell-exchange-zero-days-exploited-in-attacks/) in November as part of their Patch Tuesday updates.

However, Beaumont discovered through Shodan (http://beta.shodan.io/host/184.106.73.73) that one of Rackspace's servers, 'mex06.emailsrvr.com (http://docs.rackspace.com/support/how-to/manually-configure-outlook-2013-for-email-hosted-on-exchange-2013),' was running Microsoft Exchange build 15.0.1497.40 (https://learn.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates?view=exchserver-2019#:~:text=August%209%2C%202022-,15.0.1497.40,-15.00.1497.040), associated with the August patch level.

"This Exchange build number is from August 2022, before the ProxyNotShell patches became available," explained Beaumont in a post (http://doublepulsar.com/rackspace-cloud-office-suffers-security-breach-958e6c755d7f) about the security incident.

Shodan search query showing unpatch Microsoft Exchange servers
Source: BleepingComputer

Beaumont says that while long build numbers are not always reliable, it could be how Rackspace suffered the security incident.

BleepingComputer has reached out to Rackspace with questions about the security incident but has yet to hear back.

Update December 03, 08:31 EST: Revised the article and the title after Rackspace linked its ongoing outage to a security incident.
Update December 03, 12:38 EST: Added information from Kevin Beaumont.

Related Articles:

Rackspace confirms outage was caused by ransomware attack (https://www.bleepingcomputer.com/news/security/rackspace-confirms-outage-was-caused-by-ransomware-attack/)

Rackspace warns of phishing risks following ransomware attack (https://www.bleepingcomputer.com/news/security/rackspace-warns-of-phishing-risks-following-ransomware-attack/)

Massive Microsoft 365 outage caused by WAN router IP change (https://www.bleepingcomputer.com/news/microsoft/massive-microsoft-365-outage-caused-by-wan-router-ip-change/)

Microsoft urges admins to patch on-premises Exchange servers (https://www.bleepingcomputer.com/news/security/microsoft-urges-admins-to-patch-on-premises-exchange-servers/)

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

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

MANAGED SERVICE PROVIDER (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/MANAGED-SERVICE-PROVIDER/)

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

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

SECURITY INCIDENT (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SECURITY-INCIDENT/)

(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 (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/DHS-CYBER-SAFETY-BOARD-TO-REVIEW-LAPSUS-GANG-S-HACKING-TACTICS/)

NEXT ARTICLE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/GOOGLE-CHROME-EMERGENCY-UPDATE-FIXES-9TH-ZERO-DAY-OF-THE-YEAR/)

Comments

kalmon001 (https://www.bleepingcomputer.com/forums/u/1222903/kalmon001/) - 2 months ago

They've confirmed it was a security event. Time to look for another provider!

horsedoggs (https://www.bleepingcomputer.com/forums/u/1237488/horsedoggs/) - 1 month ago

I don’t understand why any business in would bother with hosted exchange providers such as Rackspace, in my opinion hosted exchange is primitive. Microsoft 365 is the way forward, m365 is reliable and proven when it comes to stability, scalability, security and compliance. The writing is on the wall for providers like Rackspace, they are done.

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/)

Windows Repair (All In One) (https://www.bleepingcomputer.com/download/windows-repair-all-in-one/)

Version: 4.13.1

2M+
DOWNLOADS

Everything Desktop Search (https://www.bleepingcomputer.com/download/everything-desktop-search/)

Version: 1.4.1.1017

22,118
DOWNLOADS

Zemana AntiLogger Free (https://www.bleepingcomputer.com/download/zemana-antilogger-free/)

Version: 1.8.2.320

52,703
DOWNLOADS

FOLLOW US:

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

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/)