Rackspace confirms Play ransomware was behind recent cyberattack

bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/

Sergiu Gatlan

By
Sergiu Gatlan

- January 4, 2023
- 05:21 PM
- 0

Texas-based cloud computing provider Rackspace has confirmed that the Play ransomware operation was behind a recent cyberattack that took down the company's hosted Microsoft Exchange environments.

This follows a report last month by cybersecurity firm Crowdstrike, which detailed a new exploit used by the ransomware group to compromise Microsoft Exchange servers and gain access to a victim's networks.

The exploit (dubbed OWASSRF) allowed the attackers to bypass ProxyNotShell URL rewrite mitigations provided by Microsoft by likely targeting a critical flaw (CVE-2022-41080) that allows remote privilege escalation on Exchange servers.

They also managed to gain remote code execution on vulnerable servers by abusing CVE-2022-41082, the same bug exploited in ProxyNotShell attacks.

While Crowdstrike didn't name the victim in their report, Rackspace officials have revealed in recent local media interviews and emails to BleepingComputer that the OWASSRF exploit was found on its network and Play ransomware was behind last month's ransomware attack.

"We are now highly confident that the root cause in this case pertains to a zero-day exploit associated with CVE-2022-41080. See a recent blog by CrowdStrike for more information. Microsoft disclosed CVE-2022-41080 as a privilege escalation vulnerability and did not include notes for being part of a Remote Code Execution chain that was exploitable," Karen O'Reilly-Smith, Rackspace's Chief Security Officer, told BleepingComputer.

"We thank CrowdStrike for their thorough work in discovering this zero-day exploit during the course of this investigation and will be sharing more detailed information with our customers and peers in the security community so that, collectively, we can all better defend against these types of exploits in the future."

Since the attack was discovered, Rackspace has provided customers free licenses to migrate their email from its Hosted Exchange platform to Microsoft 365.

The company is also working on providing affected users' with download links to their mailboxes (containing Hosted Exchange email data before December 2) through its customer portal via an automated queue.

"We are proactively notifying customers for whom we have recovered greater than 50% of their mailboxes," the company said on the incident report page.

"We are still working meticulously to upload the remaining data into the portal. Once available for download, the PST files will be available through the customer portal for 30 days."

Defend Exchange servers against Play ransomware attacks

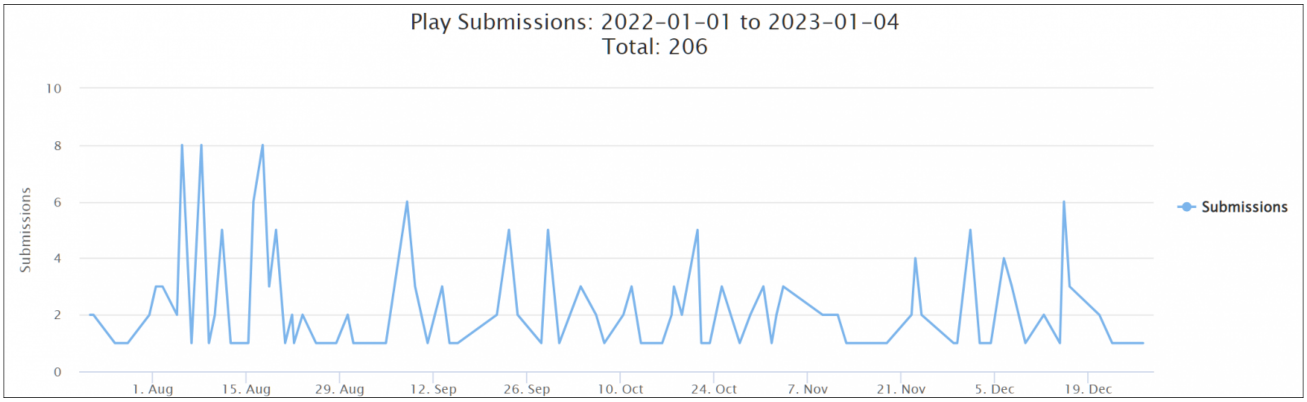
CrowdStrike said the OWASSRF exploit was used to drop remote access tools such as Plink and AnyDesk on Rackspace-compromised servers.

BleepingComputer also found that Play ransomware tooling found online by researchers also contains the ConnectWise remote administration software, which will likely be deployed in attacks.

All organizations with on-premises Microsoft Exchange servers on their network are advised to apply the latest Exchange security updates immediately (with November 2022 being the minimum patch level) or disable Outlook Web Access (OWA) until they can apply patches for CVE-2022-41080.

The Play ransomware operation was first spotted in June 2022, after the first victims began reaching out for help in the BleepingComputer forums.

Since its launch, dozens of victims have uploaded ransom notes and samples to the ID Ransomware platform to identify what ransomware was used to encrypt their files.



Play ransomware activity (ID Ransomware)

Unlike most ransomware operations, Play gang affiliates use email as a negotiation channel and will not provide victims with a link to a Tor negotiations page within ransom notes dropped on encrypted systems.

However, they are stealing data from their victims' networks before deploying ransomware payloads and will threaten to leak it online if the ransom is not paid.

Recent Play ransomware victims include the German H-Hotels hotel chain, Argentina's Judiciary of Córdoba, and the Belgium city of Antwerp.

Related Articles:

CISA orders agencies to patch Exchange bug abused by ransomware gang

Microsoft: Cuba ransomware hacking Exchange servers via OWASSRF flaw

Ransomware gang uses new Microsoft Exchange exploit to breach servers

The Week in Ransomware - December 23rd 2022 - Targeting Microsoft Exchange

The Week in Ransomware - January 13th 2023 - LockBit in the spotlight

- Microsoft Exchange

- OWASSRF
- PLAY
- Rackspace
- Ransomware

Sergiu Gatlan

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

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: