SEARCH

CATEGORIES


# QUEUEJUMPER: CRITICAL UNAUTHENTICATED RCE VULNERABILITY IN MSMQ SERVICE

April 11, 2023

**Research by:** Haifei Li.

## Executive Summary

Check Point Research recently discovered three vulnerabilities in the "Microsoft Message Queuing" service, commonly known as MSMQ. These vulnerabilities were disclosed to Microsoft and patched in the April Patch Tuesday update. The most severe of these, dubbed QueueJumper by CPR (CVE-2023-21554), is a **critical** vulnerability that could allow unauthenticated attackers to **remotely** execute arbitrary code in the context of the Windows service process mqsvc.exe.

Check Point Research (CPR) is releasing this blog after the patch was implemented to raise awareness of this critical vulnerability and provide defense insights and mitigation recommendations for Windows users. We will release the full technical details later this month, giving users time to patch their machines before publicly disclosing the technical details.

## Key Findings

- Three vulnerabilities in the MSMQ service were discovered, with all of them patched in the April Patch Tuesday update:
  - CVE-2023-21554 (QueueJumper) — unauthenticated Remote Code Execution

- CVE-2023-21769 — unauthenticated Remote Application Level DoS (service crash)
- CVE-2023-28302 — unauthenticated Remote Kernel Level DoS (Windows BSOD)

- The most significant vulnerability allows unauthenticated attackers to execute arbitrary code in the context of the Windows service process, mqsvc.exe.
- MSMQ is provided as an optional Windows component and is still available on all Windows operating systems, including the latest Windows Server 2022 and Windows 11

## MSMQ

According to Microsoft, Microsoft Message Queuing ("MSMQ" for short),

"is a message infrastructure and a development platform for creating distributed, loosely-coupled messaging applications for the Microsoft® Windows® operating system. Message Queuing applications can use the Message Queuing infrastructure to communicate across heterogeneous networks and with computers that may be offline. Message Queuing provides guaranteed message delivery, efficient routing, security, transaction support, and priority-based messaging."

The most recent Microsoft documents discussing the service were updated in 2016. Some MSMQ experts published a blog post in January 2020 exploring the retiring trend of the service. Despite being considered a "forgotten" or "legacy" service, MSMQ is still available on all Windows operating systems, including the latest Windows Server 2022 and Windows 11 and is provided as an optional Windows component. Users can easily enable the service via the Control Panel or via PowerShell command "*Install-WindowsFeature MSMQ-Services*".

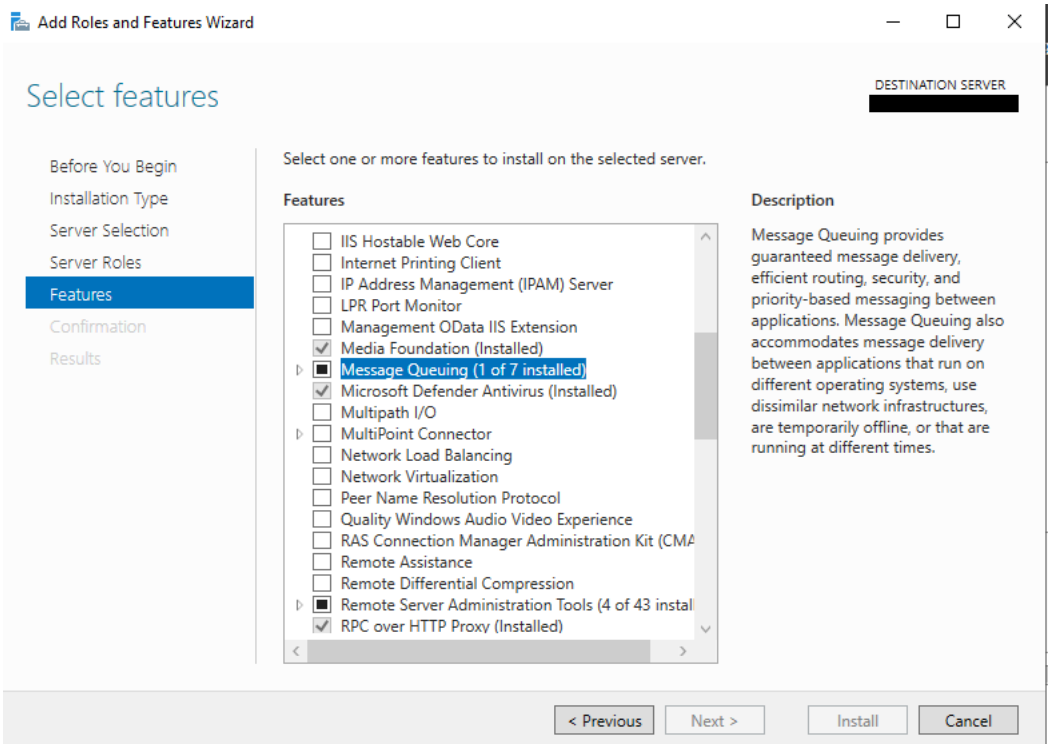


Figure 1 – Enable/disable MSMQ service on Windows server*

## The QueueJumper Vulnerability

The CVE-2023-21554 vulnerability allows an attacker to potentially execute code remotely and without authorization by reaching the TCP port 1801. In other words, an attacker could gain control of the process through just one packet to the 1801/tcp port with the exploit, triggering the vulnerability.

## The Impact

We now know the attack vector sends packets to the service port 1801/tcp. In order to have a better understanding of the potential impact in the real world of this service, CPR did a full Internet scan.

Surprisingly, we found that more than ~360,000 IPs have the 1801/tcp open to the Internet and are running the MSMQ service.

Note that this only includes the number of hosts facing the Internet and does not account for computers hosting the MSMQ service on internal networks, where the number should be far more.

The MSMQ service is a "middleware" service that some popular software relies on. When the user installs the popular software, the MSMQ service is enabled on Windows, which may be done without the user's knowledge.

For example, CPR saw that when installing the official Microsoft Exchange Server, the setup wizard app would enable the MSMQ service in the background if the user selects the "Automatically install Windows Server roles and features that are required to install Exchange" option, which is recommended by Microsoft.

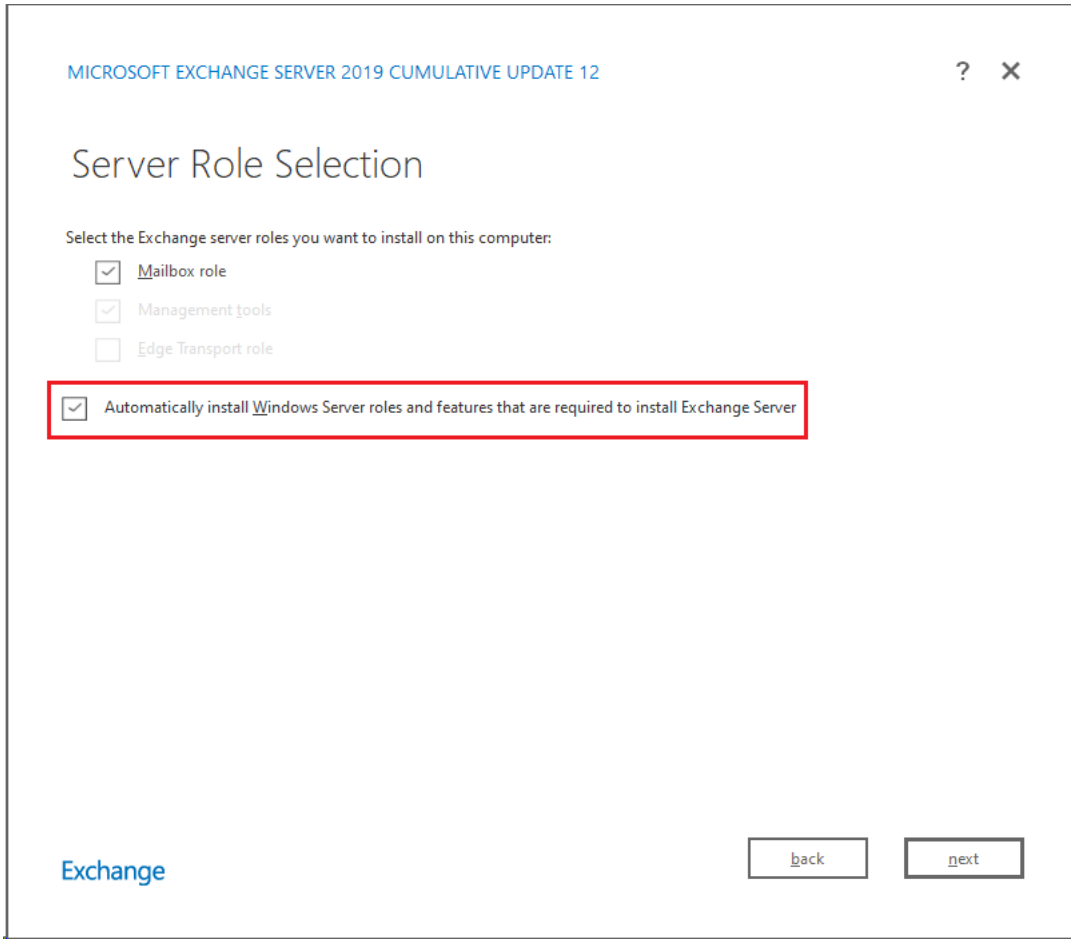


Figure 3 – Installing Exchange Server would enable MSMQ on the machine if the option is selected*

After the installation, the MSMQ service is automatically enabled:

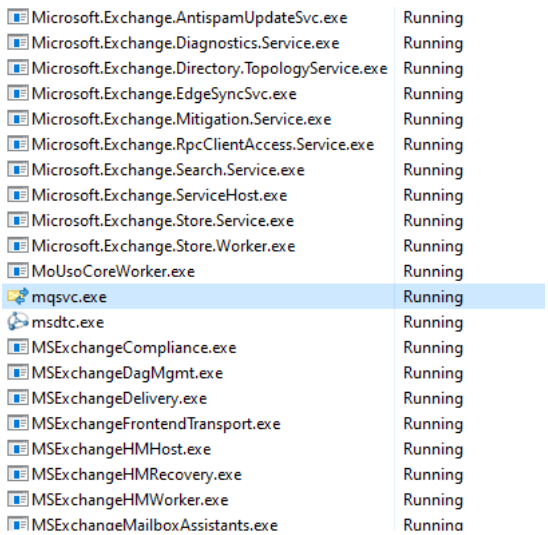

Figure 4 – After installation of Exchanger Server, MSMQ process is running on the same machine*

So, it leaves the Exchange Server running with the MSMQ service on the same machine.

The important takeaway is that if MSMQ is enabled on a server, the attacker could potentially exploit this or any MSMQ vulnerability and take over the server. Therefore, we highly recommend administrators to check their servers carefully and follow the listed protection and mitigation recommendations.

## Protection & Mitigation

We recommend all Windows admins check their servers and clients to see if the MSMQ service is installed. You can check if there is a service running named 'Message Queuing', and TCP port 1801 is listening on the computer. If it is installed, double-check if you need it. Closing unnecessary attack surfaces is always a very good security practice.

For this particular vulnerability we discussed, we recommend users install Microsoft's official patch as soon as possible. If your business requires MSMQ but is unable to apply Microsoft's patch right now, you may block the inbound connections for 1801/tcp from untrusted sources with Firewall rules (for example, blocking Internet connections to 1801/tcp for Internet-facing machines), as a workaround.

Check Point IPS has developed and deployed a signature named "**Microsoft Message Queuing Remote Code Execution (CVE-2023-21554)**" to detect and protect our customers against the QueueJumper vulnerability.

---

GO UP

BACK TO ALL POSTS

POPULAR POSTS

ARTIFICIAL INTELLIGENCE CHATGPT CHECK POINT RESEARCH PUBLICATIONS
OPWNAI : Cybercriminals Starting to Use ChatGPT

ARTIFICIAL INTELLIGENCE CHATGPT CHECK POINT RESEARCH PUBLICATIONS
OpwnAI: AI That Can Save the Day or HACK it Away

CHECK POINT RESEARCH PUBLICATIONS THREAT RESEARCH
Hacking Fortnite Accounts

BLOGS AND PUBLICATIONS

February 17, 2020

TWORKS "THE TURKISH RAT" EVOLVED ADWIND IN A MASSIVE ONGOING PHISHING CAMPAIGN

Live threat map

**About Us**

Contact Us

## Let’s get in touch

Subscribe for cpr blogs, news and more

**Subscribe Now**



Property of CheckPoint.com

Privacy Policy