For Microsoft Exchange Server Vulnerabilities, Patching Remains Patchy

Oct 06, 2021

If you've been keeping tabs on the state of vulnerabilities, you've probably noticed that Microsoft Exchange has been in the news more than usual lately. Back in March 2021, Microsoft acknowledged a series of threats exploiting zero-day CVEs in on-premises instances of Exchange Server. Since then, several related exploit chains targeting Exchange have continued to be exploited in the wild.

Microsoft quickly released patches to help security teams keep attackers out of their Exchange environments. So, what does the state of patching look like today among organizations running impacted instances of Exchange?

The answer is more mixed — and more troubling — than you'd expect.

What is Exchange, and why should you care?

Exchange is a popular email and messaging service that runs on Windows Server operating systems, providing email and calendaring services to tens of thousands of organizations. It also integrates with unified messaging, video chat, and phone services. That makes Exchange an all-in-one messaging service that can handle virtually all communication streams for an enterprise customer.

An organization's Exchange infrastructure can contain copious amounts of sensitive business and customer information in the form of emails and a type of

shared mailbox called Public Folders. This is one of the reasons why Exchange Server vulnerabilities pose such a significant threat. Once compromised, Exchange's search mechanisms can make this data easy to find for attackers, and a robust rules engine means attackers can create hard-to-find automation that forwards data out of the organization.

An attacker who manages to get into an organization's Exchange Server could gain visibility into their Active Directory or even compromise it. They could also steal credentials and impersonate an authentic user, making phishing and other attempts at fraud more likely to land with targeted victims.

Sizing up the threats

The credit for discovering this recent family of Exchange Server vulnerabilities goes primarily to security researcher Orange Tsai, who overviewed them in an August 2021 Black Hat talk. He cited 8 vulnerabilities, which resulted in 3 exploit chains:

- **ProxyLogon:** This vulnerability could allow attackers to use pre-authentication server-side request forgery (SSRF) plus a post-authentication arbitrary file write, resulting in remote code execution (RCE) on the server.
- **ProxyOracle:** With a cookie from an authenticated user (obtained through a reflected XSS link), a Padding Oracle attack could provide an intruder with plain-text credentials for the user.
- **ProxyShell:** Using a pre-authentication access control list (ACL) bypass, a PrivEsc (not going up to become an administrator but down to a user

mailbox), and a post-authentication arbitrary file write, this exploit chain could allow attackers to execute an RCE attack.

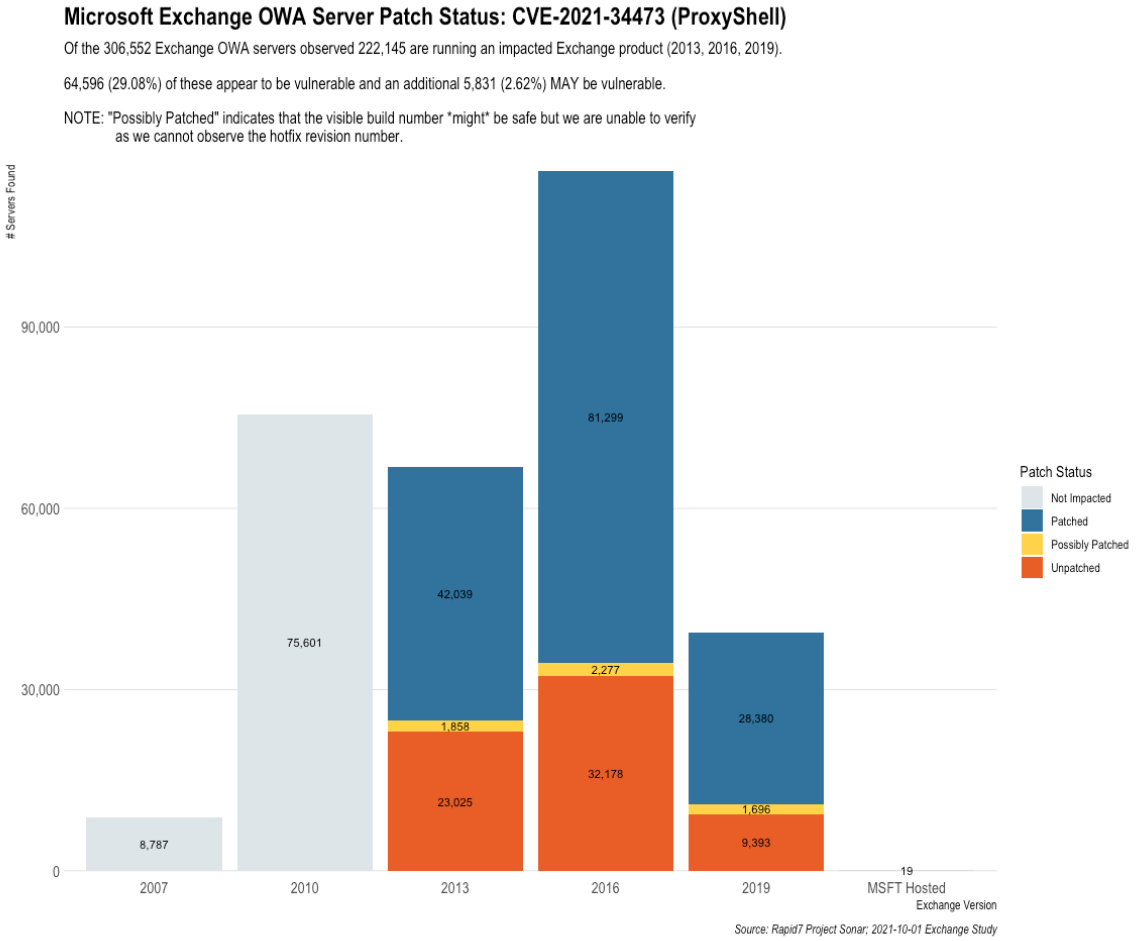
Given the sensitivity of Exchange Server data and the availability of patches and resources from Microsoft to help defend against these threats, you'd think adoption of these patches would be almost universal. But unfortunately, the picture of patching for this family of vulnerabilities is still woefully incomplete.

A patchwork of patch statuses

In Rapid7's OCTO team, we keep tabs on the exposure for major vulnerabilities like these, to keep our customers and the security community apprised of where these threats stand and if they might be at risk. To get a good look at the patch status among Exchange Servers for this family of attack chains, we had to develop new techniques for fingerprinting Exchange versions so we could determine which specific hotfixes had been applied.

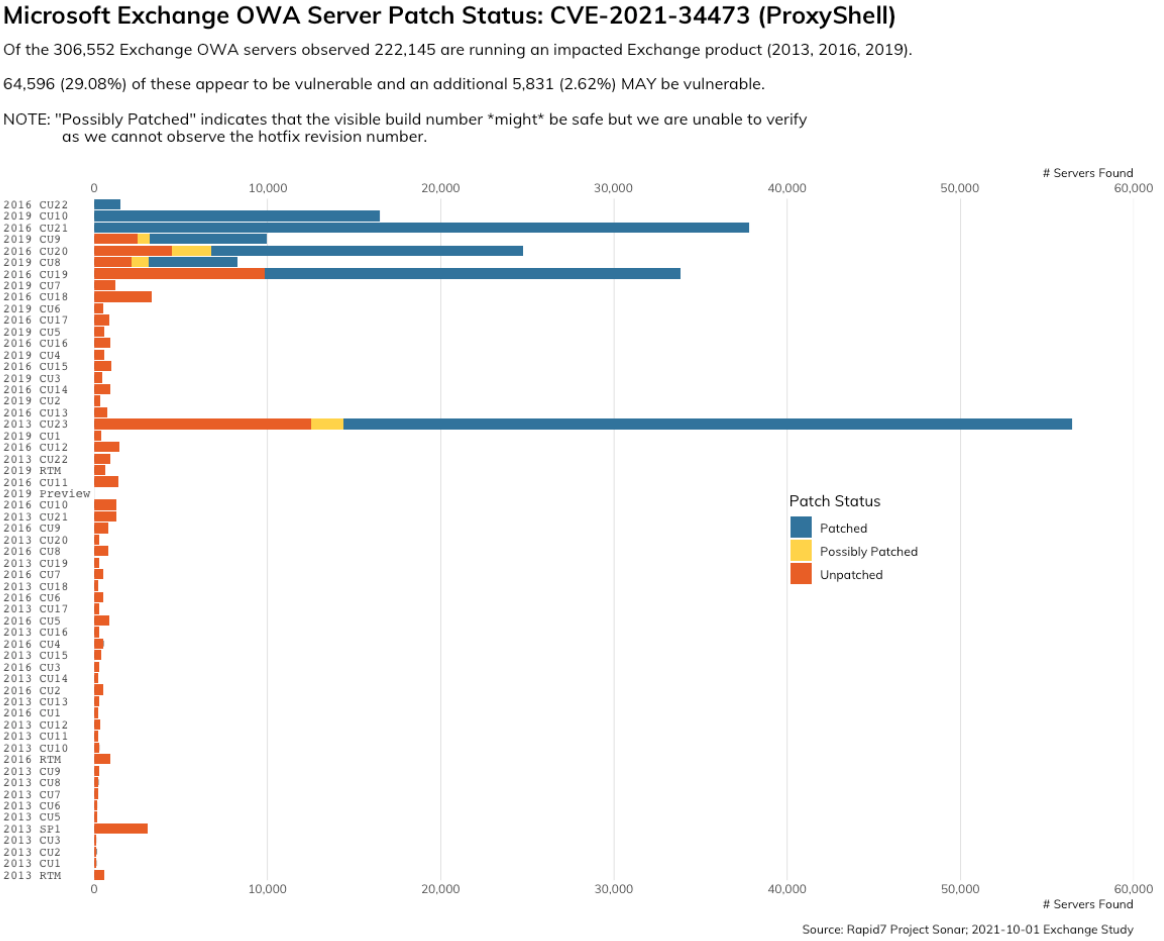
With a few tweaks, we were able to adjust our measurement approach to get a clear enough view that we can draw some strong conclusions about the patch statuses of Exchange Servers on the public-facing internet. Here's what we found:

- Out of the 306,552 Exchange OWA servers we observed, 222,145 — or 72.4% — were running an impacted version of Exchange (this includes 2013, 2016, and 2019).
- Of the impacted servers, 29.08% were still unpatched for the ProxyShell vulnerability, and 2.62% were partially patched. That makes 31.7% of servers that may still be vulnerable.

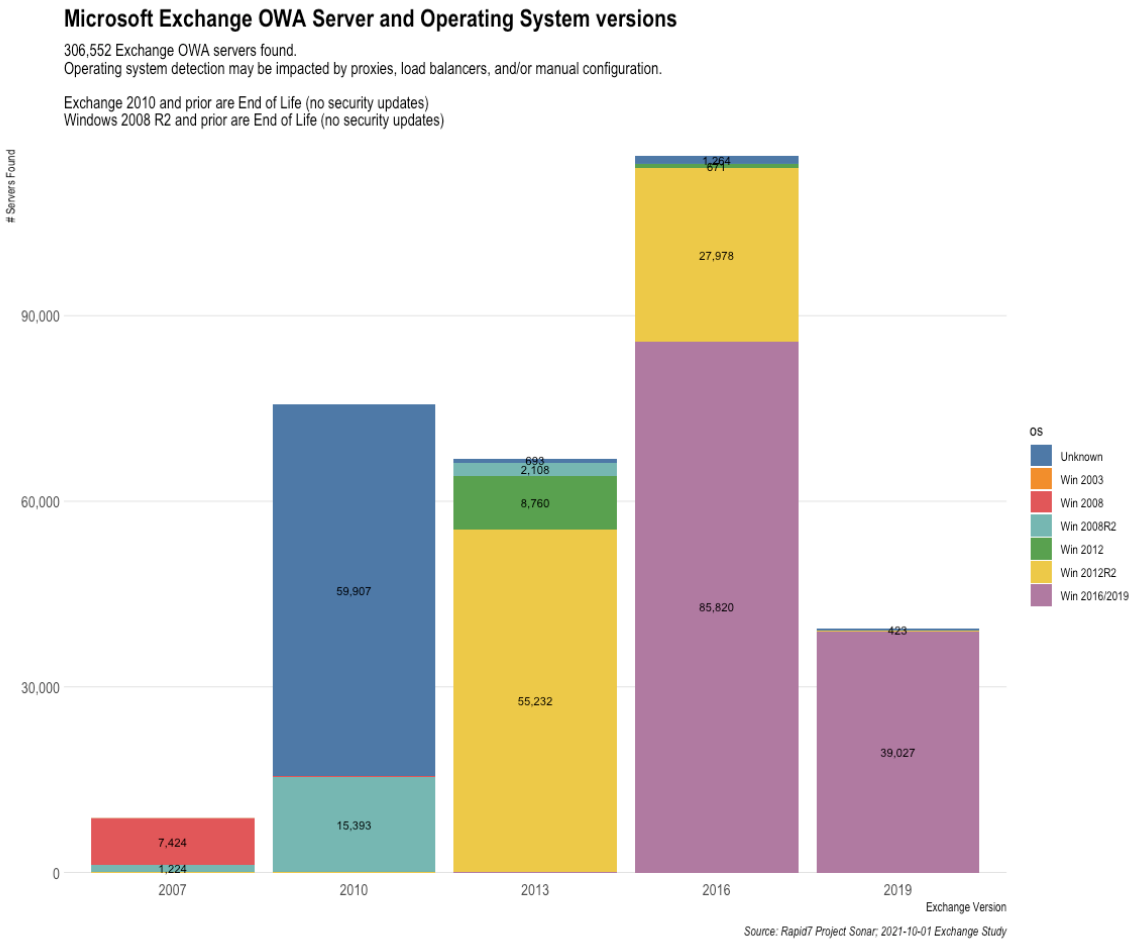


To put it another, starker way: 6 months after patches have been available for the ProxyLogon family of vulnerabilities, 1 in 3 impacted Exchange Servers are still susceptible to attacks using the ProxyShell method.

When we sort this data by the Exchange Server versions that organizations are using, we see the uncertainty in patch status tends to cluster around specific versions, particularly 2013 Cumulative Update 23.



We also pulled the server header for these instances with the goal of using the version of IIS as a proxy indicator of what OS the servers may be running — and we found an alarmingly large proportion of instances that were running end-of-life servers and/or operating systems, for which Microsoft no longer issues patch updates.



That group includes the two bars on the left of this graph, which represent 2007 and 2010 Exchange Server versions: 75,300 instances of 2010 and 8,648 instances of 2007 are still running out there on the internet, roughly 27% of all instances we observed. Organizations still operating these products can count themselves lucky that ProxyShell and ProxyLogon don't impact these older versions of Exchange (as far as we know). But that doesn't mean those companies are out of the woods — if you still haven't replaced Exchange Server 2010, you're probably also doing other risky things in your environment.

Looking ahead, the next group of products that will go end-of-life are the Windows Server 2012 and 2012 R2 operating systems, represented in green and

yellow, respectively, within the graph. That means 92,641 instances of Exchange — nearly a third of all Exchange Servers on the internet — will be running unsupported operating systems for which Microsoft isn't obligated to provide security fixes after they go end-of-life in 2023.

What you can do now

It's a matter of when, not if, we encounter the next family of vulnerabilities that lets attackers have a field day with huge sets of sensitive data like those contained in Exchange Servers. And for companies that haven't yet patched, ProxyShell and its related attack chains are still a real threat. Here's what you can do now to proactively mitigate these vulnerabilities.

- First things first: If your organization is running one of the 1 in 3 affected instances that are vulnerable due to being unpatched, install the appropriate patch right away.
- Stay current with patch updates as a routine priority. It is possible to build Exchange environments with near-100% uptimes, so there isn't much argument to be made for foregoing critical patches in order to prevent production interruptions.
- If you're running a version of Exchange Server or Windows OS that will soon go end-of-life, start planning for how you'll update to products that Microsoft will continue to support with patches. This way, you'll be able to quickly and efficiently mitigate vulnerabilities that arise, before attackers take advantage of them.

If you're already a Rapid7 customer, there's good news: InsightVM already has authenticated scans to detect these vulnerabilities, so users of the product should already have a good sense of where their Exchange environments stand. On the offensive side, your red teams and penetration testers can highlight the risk of running vulnerable Exchange instances with modules exercising ProxyLogon and ProxyShell. And as our research team continues to develop techniques for getting this kind of detailed information about exposures, we ensure our products know about those methods so they can more effectively help customers understand their vulnerabilities.

But for all of us, these vulnerabilities are a reminder that security requires a proactive mindset — and failing to cover the basics like upgrading to supported products and installing security updates leaves organizations at risk when a particularly thorny set of attack chains rears its head.