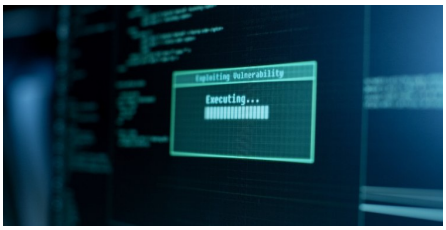
If you purchase via links on our site, we may receive affiliate commissions.

Millions of Microsoft web servers powered by vulnerable legacy software

by Edvardas Mikalauskas 09 September 2021 1



- Millions of Microsoft web servers are running on unsupported and vulnerable versions of IIS
- More than a million still use an IIS version that had been discontinued by Microsoft last year
- Most servers are located in Asia and North America

CyberNews researchers identified more than 2 million web servers worldwide still running on outdated and vulnerable versions of Microsoft Internet Information Services software. These legacy versions are no longer supported by Microsoft, which makes millions of web servers easy targets for threat actors and cybercriminals.

Boasting a market share of 12.4%, Microsoft Internet Information Services (IIS) is the third-most-popular suite of web server software, used to power at least 51.6 million websites and web applications worldwide. When it comes to security, most web servers running the latest versions of IIS will generally be in good shape.

However, not all versions of IIS are created equal.

While Microsoft keeps the newer versions relatively safe by releasing security updates and vulnerability hotfixes, older IIS versions from 7.5 downwards are no longer supported by the company. And like other types of outdated server software, all legacy versions of Microsoft IIS suffer from numerous critical security vulnerabilities.

This means that any website that runs on an unsupported IIS version is a lucrative target for threat actors, allowing them to easily infiltrate such sites, inject them with dangerous malware, and steal their visitors' data, including login and payment information.

With that in mind, we at CyberNews decided to find out how many web servers are still powered by discontinued versions of Microsoft IIS, making them sitting ducks for cybercriminals.

How we collected and analyzed the data

In order to conduct this investigation, we identified five different versions and subversions of IIS that have been discontinued by Microsoft and matched them with known Common Vulnerabilities and Exposures (CVEs) associated with those versions.

We then used an IoT search engine to look for open unpatched IIS web servers that were susceptible to known CVEs and investigated the results for statistical data.

From the initial results, we filtered out honeypots, which are decoy services or systems set up by security teams and researchers as bait for threat actors.

Here's what we found.

2 million Microsoft IIS servers are vulnerable to threat actors

During our investigation, we identified 7,335,868 potentially vulnerable web servers across the world running legacy versions of IIS.

While 72% of these servers were honeypots used as bait by researchers and security teams, more than 2 million of the instances we discovered were actually running on vulnerable software that is no longer supported by Microsoft.

According to CyberNews security researcher Mantas Sasnauskas, since web servers that host public websites must be publicly accessible to function, they are also broadcasting their outdated IIS versions for everyone to see.

> *"This means that running these servers on visibly vulnerable software is tantamount to extending an invitation to threat actors to infiltrate their networks."*
>
> *- CyberNews security researcher Mantas Sasnauskas*

Terumi Laskowsky, a cybersecurity instructor at DevelopIntelligence, argues that having so many vulnerable web servers in the open makes it incredibly easy for threat actors to perform reconnaissance. "If there are millions of unpatched IIS servers, the attackers feel like kids in a candy store," Laskowsky told CyberNews.

Being aware of a web server's vulnerabilities, threat actors can quickly collect data about the best way to attack the target.

"Knowing the description and severity of a vulnerability is just one step in a series of steps that lead to the actual attack. The next logical step is to find ways to launch the attack. There are plenty of free sites that give this information, too," says Laskowsky. "Not all attacks will succeed, but enough will to make the effort worthwhile for the attackers."

Most vulnerable IIS web servers are located in China

Our investigation shows that mainland China tops the list of vulnerable server locations with 679,941 exposed instances running legacy versions of IIS. Meanwhile, 581,708 unprotected servers reside in the US, which runs a close second.

Hong Kong, where we identified 203,786 vulnerable IIS servers, comes third, while South Korea and Germany round out the top five with 54,981 and 43,857 servers, respectively.

According to Andrew Useckas, CTO at ThreatX, China's staggering numbers could be explained by the country's lax stance on software piracy and the massive proliferation of bootleg Windows copies throughout China.

"The reason why there are so many Microsoft IIS servers in China is the same reason why there are so many of them in Russia. It's easier to install than Linux servers, and license costs are of no issue since these are mostly bootleg versions of Windows," says Useckas. "Of course, it's typical that the people who install these pirated versions have no idea how to maintain them and could not be bothered to upgrade them."

Ben Carr, CISO of Qualys, adds that the meteoric pace of China's economy may be another reason behind the massive number of unsecured web servers across the country.

According to Carr, organizations based in Western countries have more regulations and compliance to follow in their markets, while publicly traded companies have fiduciary responsibilities to their shareholders. He believes that this forces companies to invest more time and resources into security as they develop and grow their operations.

"That process is still developing in China, where the rules are more about market access at the moment. As the economy there matures, there should be more compliance and security guidance in place for them to follow," says Carr.

The most vulnerable IIS version

In effect, every single legacy version of Microsoft IIS is susceptible to at least five known vulnerabilities, most of them critical and relatively easily exploitable by experienced threat actors.

However, version 7.0 is the most vulnerable version of Microsoft IIS, being susceptible to 17 known vulnerabilities according to itsecdb.com. We identified 47,620 legacy web servers running on this version of IIS.

1.4 million vulnerable servers run IIS version 7.5

On the other hand, version 7.5, which was discontinued by Microsoft on January 14, 2020, seems to be by far the most popular Microsoft IIS version run by the vulnerable servers, dwarfing the others by orders of magnitude with a grand total of 1,376,216 instances across the web.

Version 6.0 lags relatively far behind the frontrunner with 167,870 vulnerable web servers, with most of them located in China. Version 7.0, the most vulnerable of the bunch, sits in third with 47,620 exposed servers in the wild, and 47% of them are based in the US.

The prevalence of IIS version 7.5 might be explained by the fact that it was discontinued relatively recently. According to Drew Pilarski, Security Engineer at oak9, upgrading to the latest versions of software takes time and money, and not everyone is willing to incur the costs of the transition as soon as a certain version reaches its end of life.

"Patching takes time in regard to planning and testing patches, costs money, and can lead to application behavior changes that require development changes," says Pilarski. "Without a clear understanding of the risks of unpatched software, many developers determine that the costs of patching are greater than the benefits."

Keep your software up to date: it's worth the hassle

If you're at least somewhat security-minded, keeping your software up to date might seem like a no-brainer. And yet, simple doesn't mean easy. This is especially true for web developers who have to juggle multiple responsibilities at the same time, and maintaining software versions sometimes ends up relatively low on their priority list.

According to Ben Carr, developers are incentivised to focus on new features rather than on existing applications and their maintenance. "Normally, people think of maintenance as something that takes away from productive time - you aren't working on new features, and actually you are spending your time away from what will make your company more revenue in the future," Carr told CyberNews.

"However, that is a false economy. The impact of a breach is significant, so you should budget for maintenance and fixes both in your technology and mentality, as part of how your team approaches this in the first place."

John Riganati, a senior executive advisor at Think Systems, adds that developers need to start working hand in hand with systems and security professionals.

"Protecting and securing web-facing environments is a profession unto itself. But developers can't just throw their code over the proverbial wall and expect security teams to work out the rest," says Riganati. "The first thing is to know what you have. For web developers, have a software bill of materials and keep up with what you have developed in the past. This makes it easier to know what you have implemented previously, any dependencies that you might have, and what you have to fix over time."

Riganati argues that web developers should also take into account the full lifecycle of an application when they carry out their planning. He believes they should maintain the full inventory of systems that are providing services and have a plan for their maintenance over the lifecycle.

"This includes areas like IT management, patching the application, carrying out updates and coding fixes, until you sunset the service. You should factor this into your development costs, budgets, and financial overheads from the start. Too many times, the budget gets put towards new development alone," Riganati told CyberNews.

> *"The biggest piece of advice? Patch your stuff, so you won't be sorry."*
>
> *- Think Systems senior executive advisor John Riganati*

Share Tweet Share Share Share

Comments

Scott Williams 3 days ago
How did you figure out which servers were honeypots? That's a very interesting stat, that so many are being used this way.

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name * **Email ***

Privacy Policy Agreement *

I agree to the Terms & Conditions and Privacy Policy.

Post comment

Editor's choice

EDITORIAL

It seems I bought a PS4 for $1000: Ambien shopping or a scam?

by Jurgita Lapienytė 08 September 2021

I've always wanted a PlayStation. And if I hadn't already bought one during the peak of recent quarantine boredom, I...

Read more

Infamous ransomware gangs are rebranding and preparing to strike
07 September 2021

Bill of materials: devil's in the software details
06 September 2021

ProtonMail shared activist's IP with law enforcement, claims had no other choice
06 September 2021

'Amazon's Choice' best-selling TP-Link router ships with vulnerable firmware
02 September 2021

CATEGORIES
News
Editorial
Security
Privacy
Crypto
Cloud

REVIEWS
Antivirus Software
Password Managers
Best VPN Services
Secure Email Providers
Website Builders
Best web hosting services

TOOLS
Password generator
Personal data leak checker
Password leak checker

ENGAGE
About Us
Send Us a Tip
Careers

About Us Contact Send Us a Tip Privacy Policy Terms & Conditions Vulnerability Disclosure

© 2021 CyberNews - Latest tech news, product reviews, and analyses.

This website uses cookies. By continuing to use this website you are giving consent to cookies being used. Visit our Privacy Policy. I Agree