

Navigating Microsoft Security Update Resources

A Comprehensive Handbook

CSS Security Regional PM team



Revisions notes

Version	Date	Notes
1.0	May 14, 2024	Document published.

Objective

- This document provides a comprehensive guide on Microsoft Security Updates resources.
- Target Audience
 - IT professionals who needs to manage Microsoft Products
 - Security responders who needs to assess risks associated with Microsoft products
 - Security evangelists who wants to understand Microsoft security updates

1. Tracking Microsoft Security Vulnerabilities & Security Updates Publications

Microsoft Security Vulnerabilities & Security Updates Publications

Microsoft publishes security updates information at the following places.

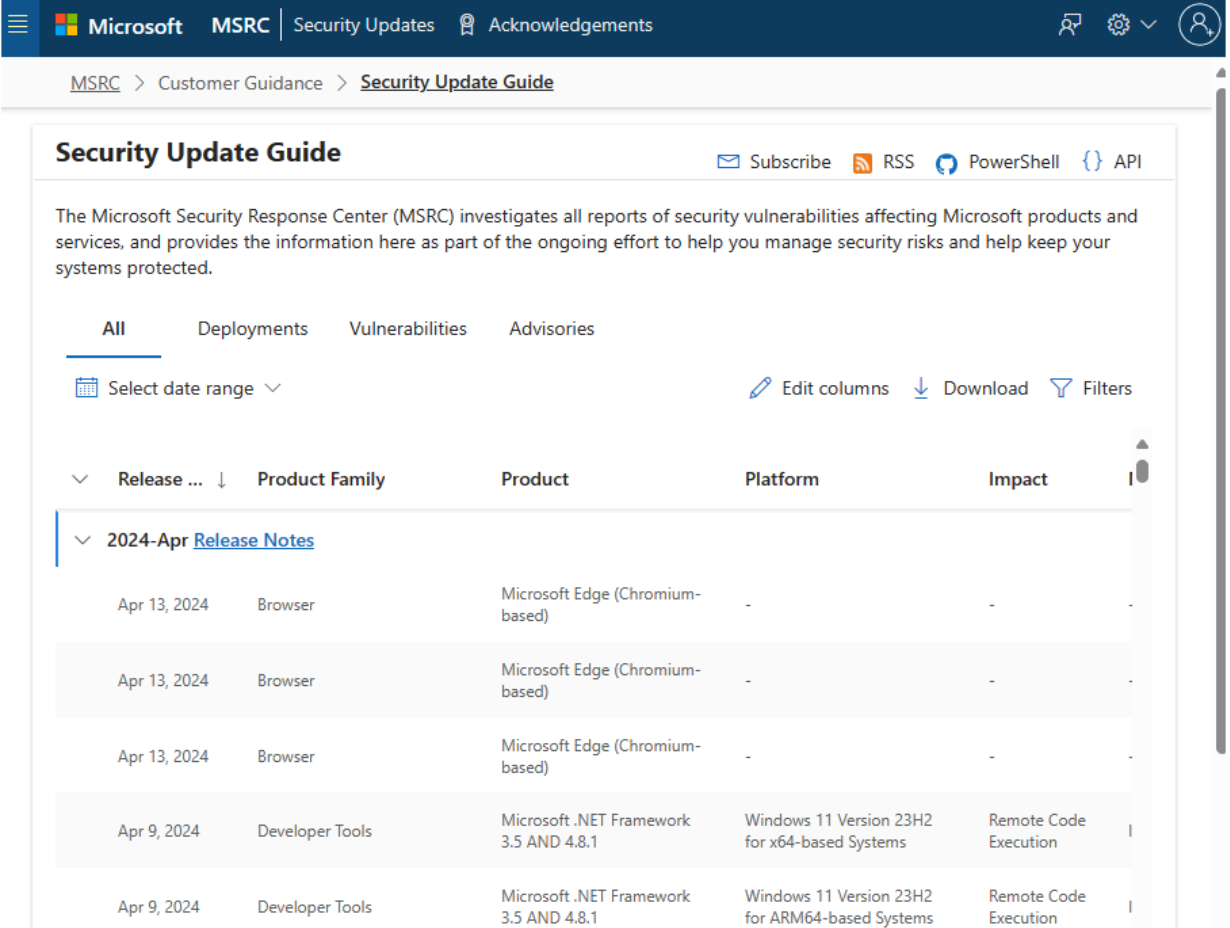
Who	Microsoft Security Response Center	Microsoft Update Windows Update	Product Groups	Microsoft Security
What	<ul style="list-style-type: none">• Microsoft vulnerability information	<ul style="list-style-type: none">• Update packages• Automatic updates delivery	<ul style="list-style-type: none">• Product release notes• Update deployment guidance	<ul style="list-style-type: none">• Detection and protection guidance• Vulnerability exploitation details
Where	<ul style="list-style-type: none">• Security Update Guide – Microsoft• Microsoft Security Response Center	<ul style="list-style-type: none">• Microsoft Update Catalog	<ul style="list-style-type: none">• Knowledge Base (KB) articles• Product team blogs	<ul style="list-style-type: none">• Microsoft Security Blog

Publications by Microsoft Security Response Center

Security Update Guide

<https://msrc.microsoft.com/update-guide>

- The Microsoft Security Update Guide (SUG) is the authoritative source of information for Microsoft security vulnerability.
- It serves as a comprehensive resource for IT professionals, helping them understand and utilize Microsoft's security release information, processes, communications, and tools.
- By referring to the SUG, IT teams can effectively manage organizational risk and establish a repeatable, efficient deployment mechanism for security updates.



Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.

Release ...	Product Family	Product	Platform	Impact
2024-Apr Release Notes				
Apr 13, 2024	Browser	Microsoft Edge (Chromium-based)	-	-
Apr 13, 2024	Browser	Microsoft Edge (Chromium-based)	-	-
Apr 13, 2024	Browser	Microsoft Edge (Chromium-based)	-	-
Apr 9, 2024	Developer Tools	Microsoft .NET Framework 3.5 AND 4.8.1	Windows 11 Version 23H2 for x64-based Systems	Remote Code Execution
Apr 9, 2024	Developer Tools	Microsoft .NET Framework 3.5 AND 4.8.1	Windows 11 Version 23H2 for ARM64-based Systems	Remote Code Execution

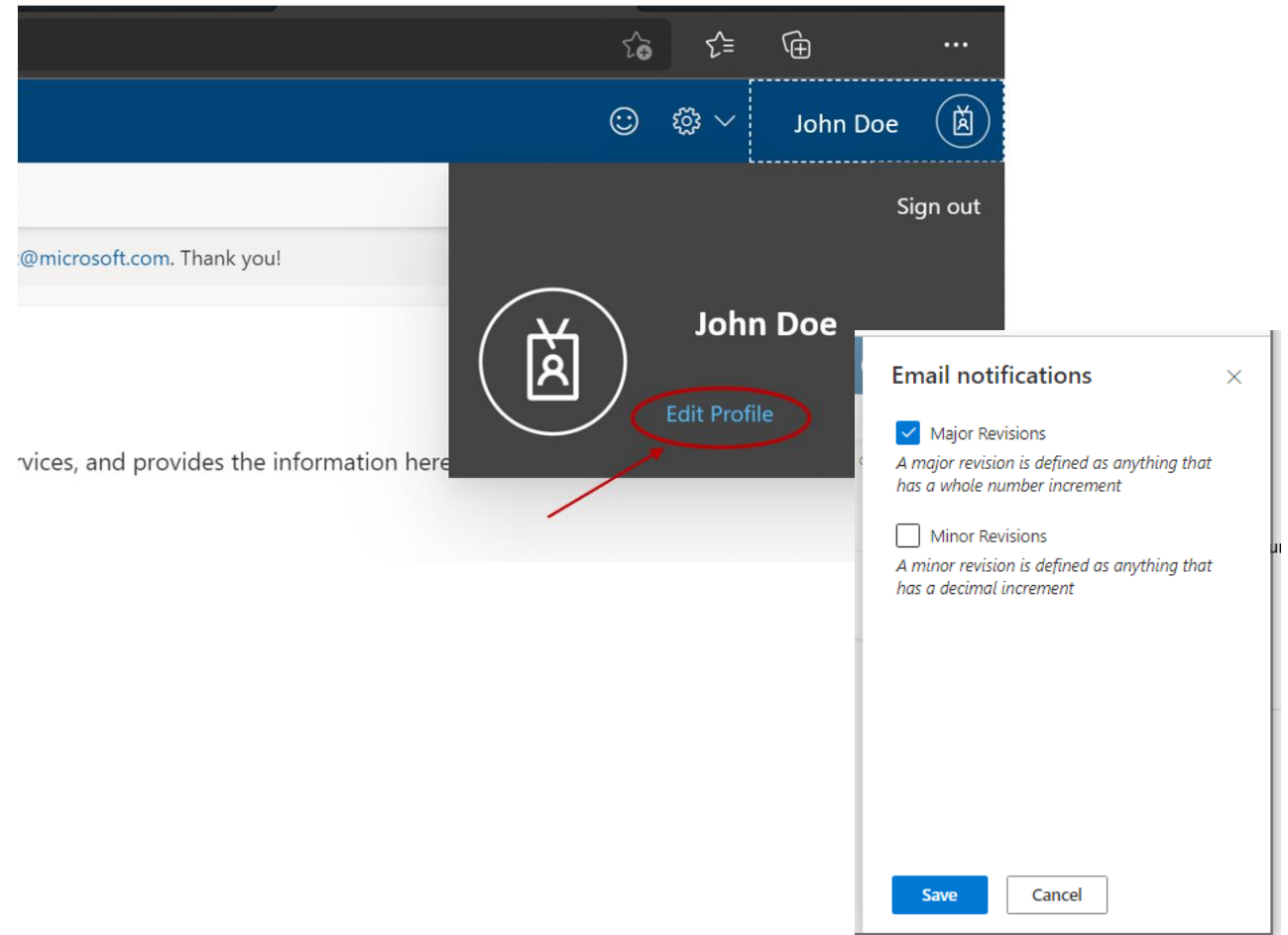
Security Update Guide: Notifications

- By signing up for notifications, you can receive them at the email address of your choice.
- Types of notifications
 - **Major updates:** Only Major updates are notified. Major updates include new CVEs that are published and existing CVEs that are republished due to a change in software updates in the Security Updates table. Major updates are marked with an incremented initial number such as 1.0, 2.0, etc.
 - **All updates:** All updates including Minor updates are notified. Minor updates are changes to FAQs or Acknowledgements or other informational type revisions. Minor updates are marked with an incremented final number such as 1.1, 3.2, etc.
- Read more at: [Security Update Guide Notification System News: Create your profile now – Microsoft Security Response Center](#)

Security Update Guide: Notification set up

Steps to set notifications

1. Click the Profile and sign in. You will know you have successfully signed in when your Profile name is displayed.
2. Click on your Profile name and then select Edit Profile in the pop-up menu.
3. Click Edit on the Email notifications column to select the type of notifications you would like to receive.
4. Click Save when you're finished.



Security Update Guide: APIs

- The Microsoft [Security Update Guide](#) is the web experience to find security update detail. Microsoft provides an API for programmatic access to security update details using [Common Vulnerability Reporting Format](#). See [Furthering our commitment to security updates](#) for details.
- Security Update API information on GitHub:
<https://github.com/microsoft/MSRC-Microsoft-Security-Updates-API>
 - This repository contains sample code and documentation for the Microsoft Security Updates API (<https://portal.msrc.microsoft.com/en-us/developer>), including:
 - source code for the [MsrcSecurityUpdates PowerShell module](#)
 - sample code for using the [MsrcSecurityUpdates PowerShell module](#)
 - OpenAPI/Swagger definition for the Microsoft Security Updates API

Microsoft Security Response Center Blog

- The MSRC's mission is to protect customers, communities, and Microsoft by addressing current and emerging security and privacy threats. They work tirelessly to identify the root causes of security vulnerabilities in Microsoft products and services.
- The MSRC shares valuable insights through blogs, conferences (such as BlueHat), and reports, enhancing security awareness and knowledge.

- [Microsoft Security Response Center Blog](#)


- Microsoft Security Response Center SNS



[@msftsecresponse](#)



[Microsoft Security Response Center](#)

 | MSRC [Report an issue](#) [Customer guidance](#) [Engage](#) [Who we are](#) [Blogs](#) [Acknowledgments](#)

Blog /

Microsoft Security Response Center Blog

[Congratulations to the Top MSRC 2024 Q1 Security Researchers!](#)

Wednesday, April 17, 2024

Congratulations to all the researchers recognized in this quarter's Microsoft Researcher Recognition Program leaderboard! Thank you to everyone for your hard work and continued partnership to secure customers. The top three researchers of the 2024 Q1 Security Researcher Leaderboard are Yuki Chen, VictorV, and Nitesh Surana! Check out the full list of researchers recognized this quarter here.

[Read More >](#)

[Researcher Recognition](#) [Security Research](#) [Community-Based Defense](#) [Security Researcher](#)

[Toward greater transparency: Adopting the CWE standard for Microsoft CVEs](#)

Monday, April 08, 2024

At the Microsoft Security Response Center (MSRC), our mission is to protect our customers, communities, and Microsoft from current and emerging threats to security and privacy. One way we achieve this is by determining the root cause of security vulnerabilities in Microsoft products and services. We use this information to identify vulnerability trends and provide this data to our Product Engineering teams to enable them to systematically understand and eradicate security risks.

[Read More >](#)

[Security Update Guide](#)

[Embracing innovation: Derrick's transition from banking to Microsoft's Threat Intelligence team](#)

Tuesday, April 02, 2024

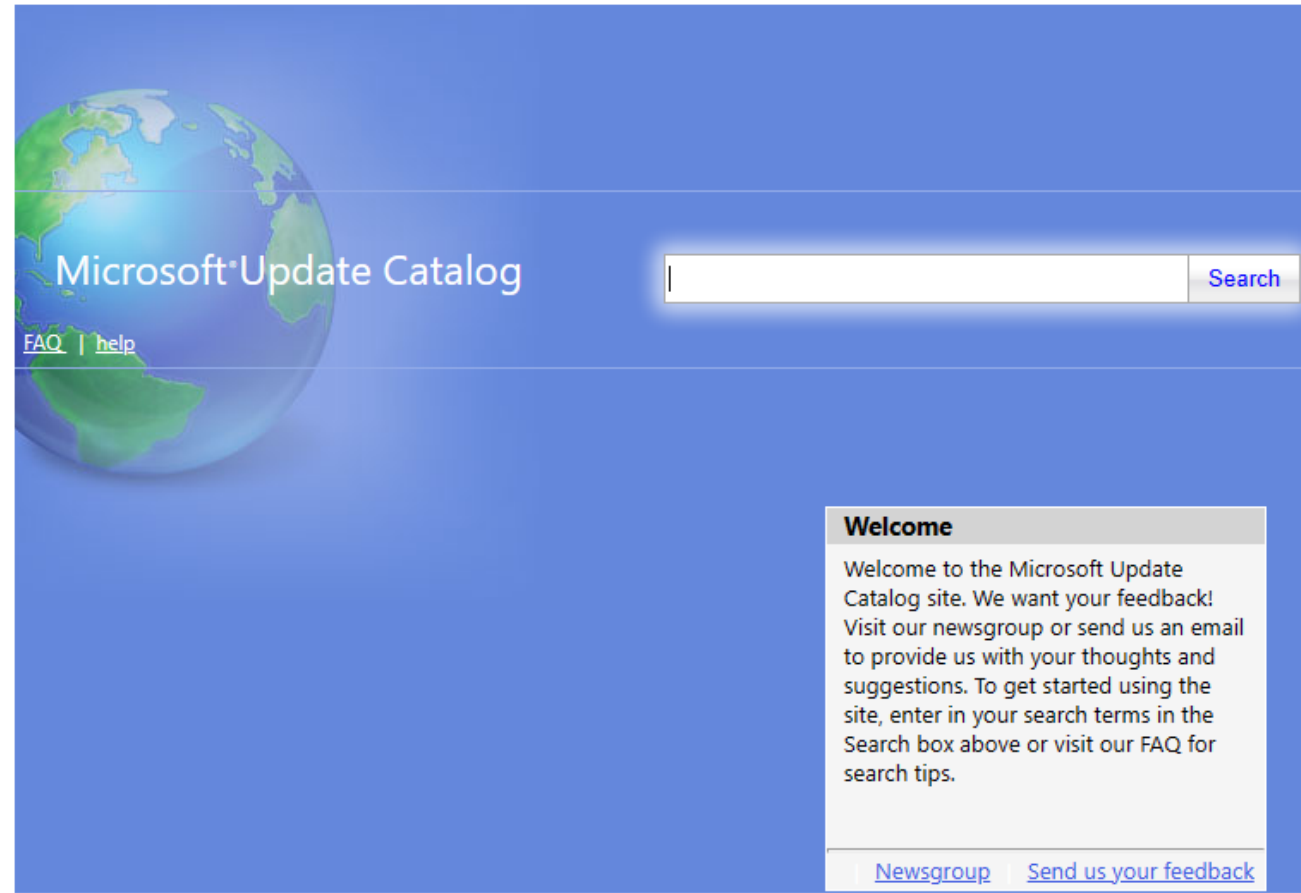
Meet Derrick, a Senior Program Manager on the Operational Threat Intelligence team at Microsoft. Derrick's role involves

**Publications by
Microsoft Update / Windows Update**

Microsoft Update Catalog

- Microsoft Update Catalog provides a listing of updates that can be distributed over a corporate network. You can use it as a one-stop location for finding Microsoft software updates, drivers, and hotfixes.

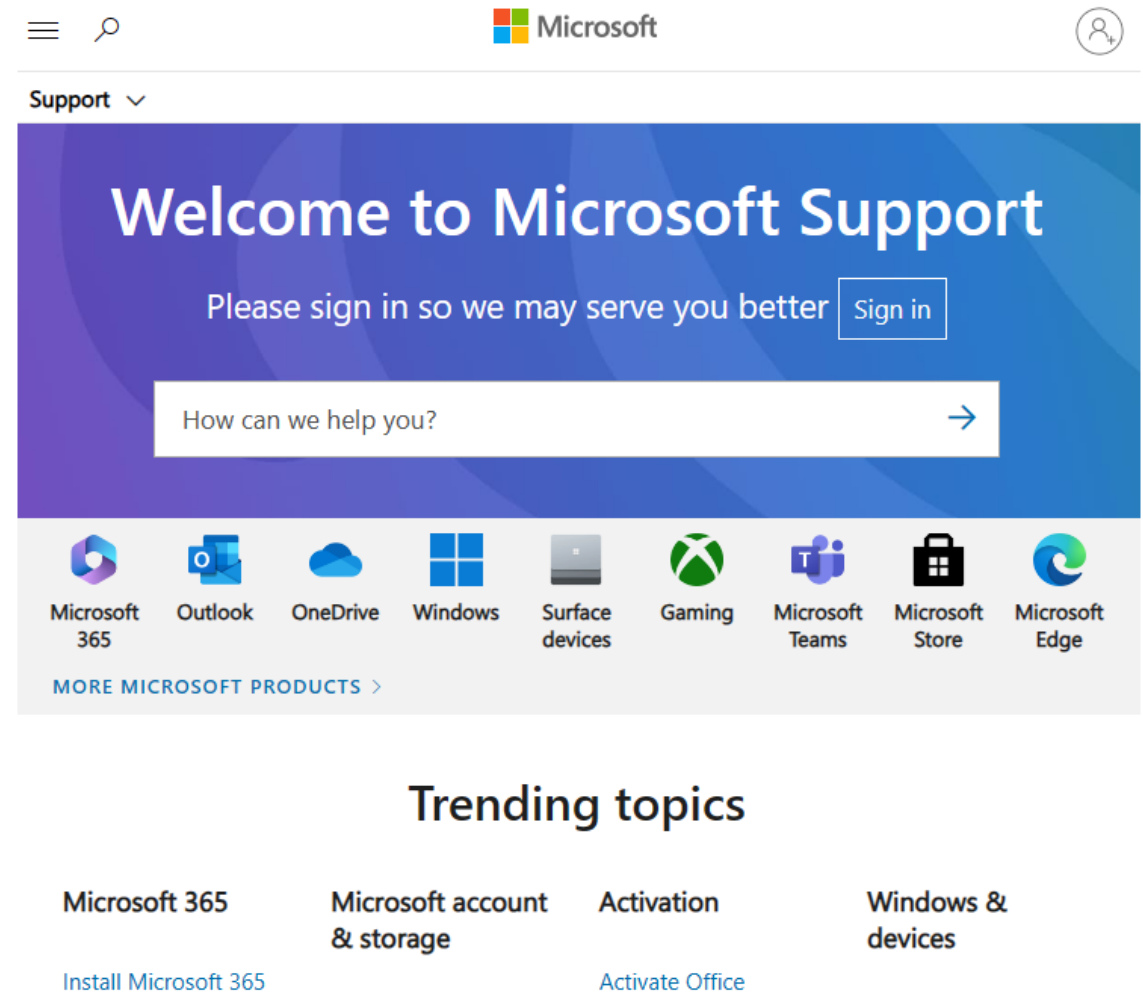
[Microsoft Update Catalog](https://www.catalog.update.microsoft.com/)



Publications by Product Teams

Knowledge Base (KB) articles

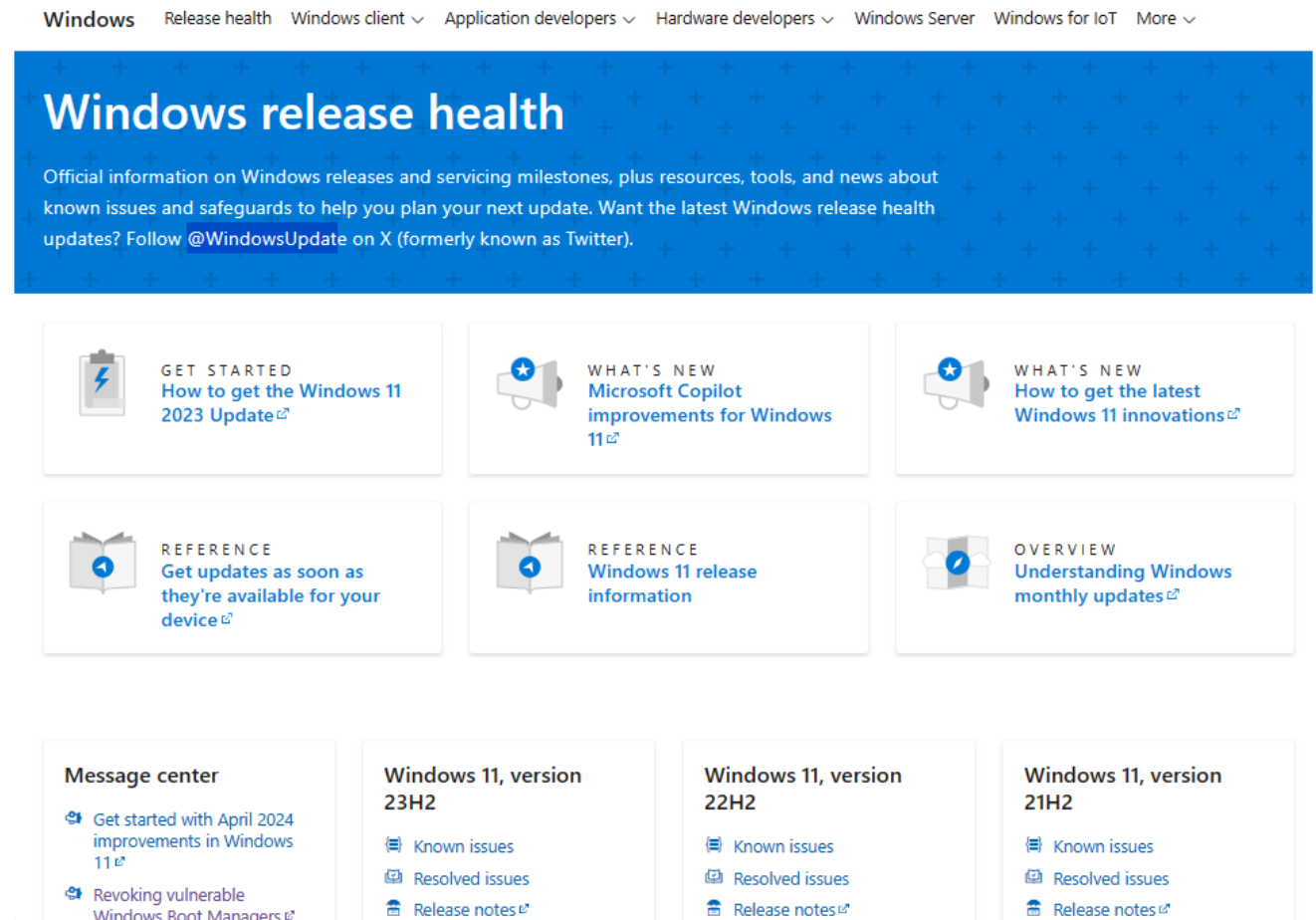
- Microsoft provides Knowledge Base (KB) articles that link to the corresponding security updates without duplicating the same information in the Security Update Guide.
- KB articles are also released to highlight known issues with security updates and will continue to be refreshed.
- [Description of Software Update Services and Windows Server Update Services changes in content for 2024 \(KB894199\) - Microsoft Support](#)



[Windows] Windows Release Health

- [Windows release health](#)
- Official information on Windows releases and servicing milestones, plus resources, tools, and news about known issues and safeguards to help you plan your next update.

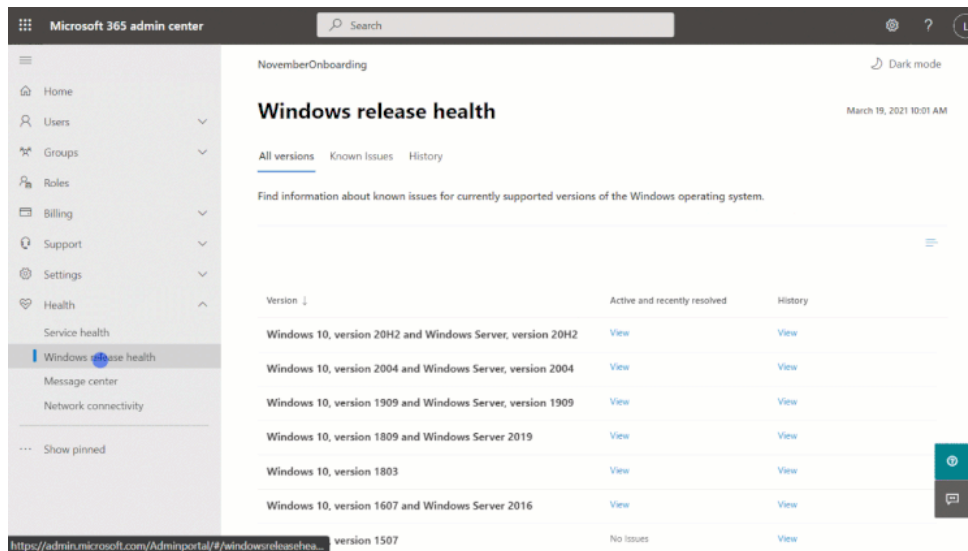
 [@WindowsUpdate](#)



The screenshot shows the 'Windows release health' page. At the top is a navigation bar with links: Windows, Release health, Windows client, Application developers, Hardware developers, Windows Server, Windows for IoT, and More. The main header is 'Windows release health' with a subtitle: 'Official information on Windows releases and servicing milestones, plus resources, tools, and news about known issues and safeguards to help you plan your next update. Want the latest Windows release health updates? Follow @WindowsUpdate on X (formerly known as Twitter).' Below this are six tiles: 'GET STARTED How to get the Windows 11 2023 Update', 'WHAT'S NEW Microsoft Copilot improvements for Windows 11', 'WHAT'S NEW How to get the latest Windows 11 innovations', 'REFERENCE Get updates as soon as they're available for your device', 'REFERENCE Windows 11 release information', and 'OVERVIEW Understanding Windows monthly updates'. At the bottom are four columns: 'Message center' (with links for April 2024 improvements and revoking vulnerable boot managers), 'Windows 11, version 23H2' (with links for known issues, resolved issues, and release notes), 'Windows 11, version 22H2' (with links for known issues, resolved issues, and release notes), and 'Windows 11, version 21H2' (with links for known issues, resolved issues, and release notes).

[M365] Windows release health in the admin center

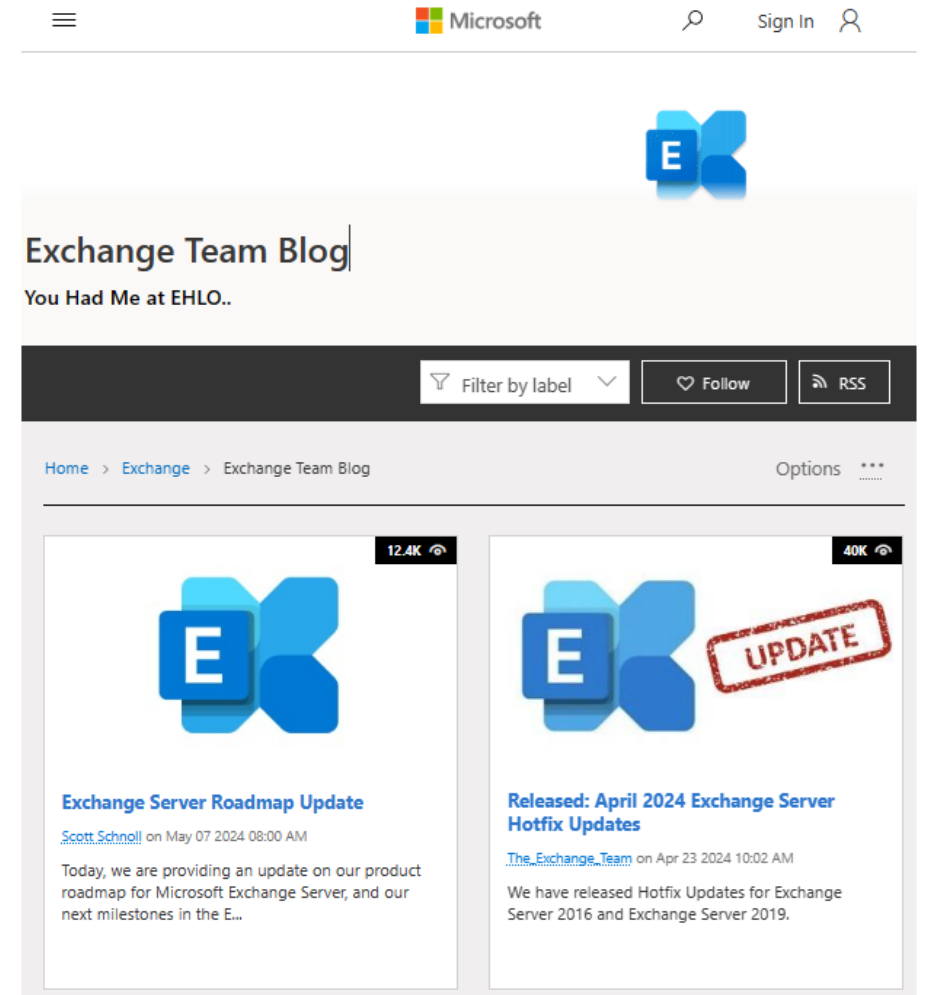
- Windows and Microsoft 365 IT admins now have easy, integrated access to essential information about monthly quality and feature updates, the latest features and enhancements for IT, servicing milestones, and lifecycle updates.
- The Windows release health experience on the admin center also offers insights into known issues, workarounds, and resolutions related to Windows updates.



- visit <https://admin.microsoft.com>, log in, and scroll down to Health in the navigation menu. Windows release health will be listed underneath the existing Service health menu option.
- In order to access Windows release health in the admin center, you will need an applicable Microsoft 365 or Windows licensing subscription, and to have the role of Service support admin for your tenant.
- Read more at [How to check Windows release health](#)

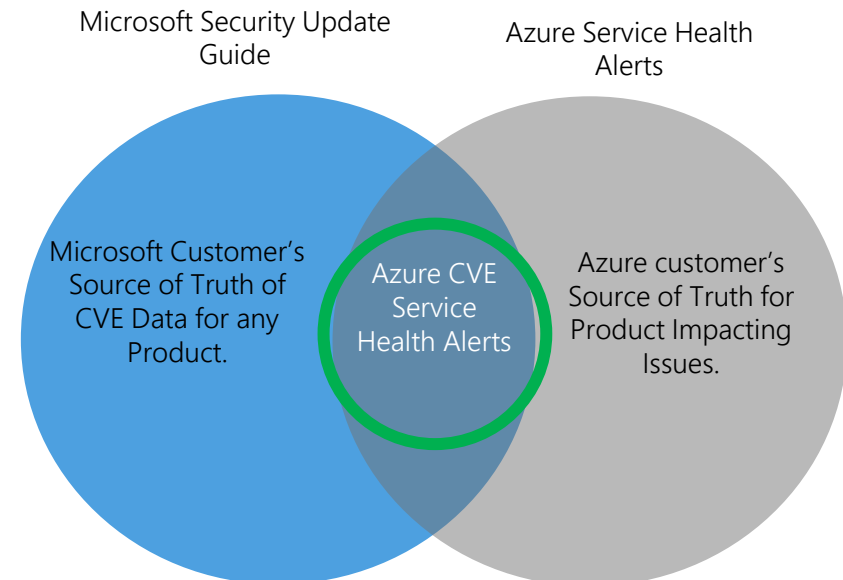
[Microsoft Exchange] Exchange Team Blog

- The Exchange Team Blog is a valuable resource for staying informed about all things related to Microsoft Exchange.
 - Product roadmaps and announcements
 - Monthly Security Updates deployments
- [Exchange Team Blog - Microsoft Community Hub](#)



[Azure] Azure Service Health

- When a vulnerability is disclosed that affects their resources, customers will be notified through [Service Health](#) in the Azure Portal.
- This Service Health message will include information about the vulnerability's common vulnerabilities and exposures number (CVE), severity, and steps customers can take to safeguard against it. In most cases, it will also include a list of the specific resources in their subscription that customers need to take action on.
- Learn more at
 - [Understanding Service Health communications for Azure vulnerabilities](#)
 - [Azure Service Health Overview](#)
 - [Stay informed about Azure security issues - Azure Service Health](#)



Other Product Team Blogs

- [Microsoft SQL Server Blog | News and Best Practices](#)
- [Microsoft SharePoint Blog - Microsoft Community Hub](#)
- [Microsoft 365 Blog | Latest Product Updates and Insights](#)
- [Microsoft Teams Blog - Microsoft Community Hub](#)
- [.NET Blog \(microsoft.com\)](#)

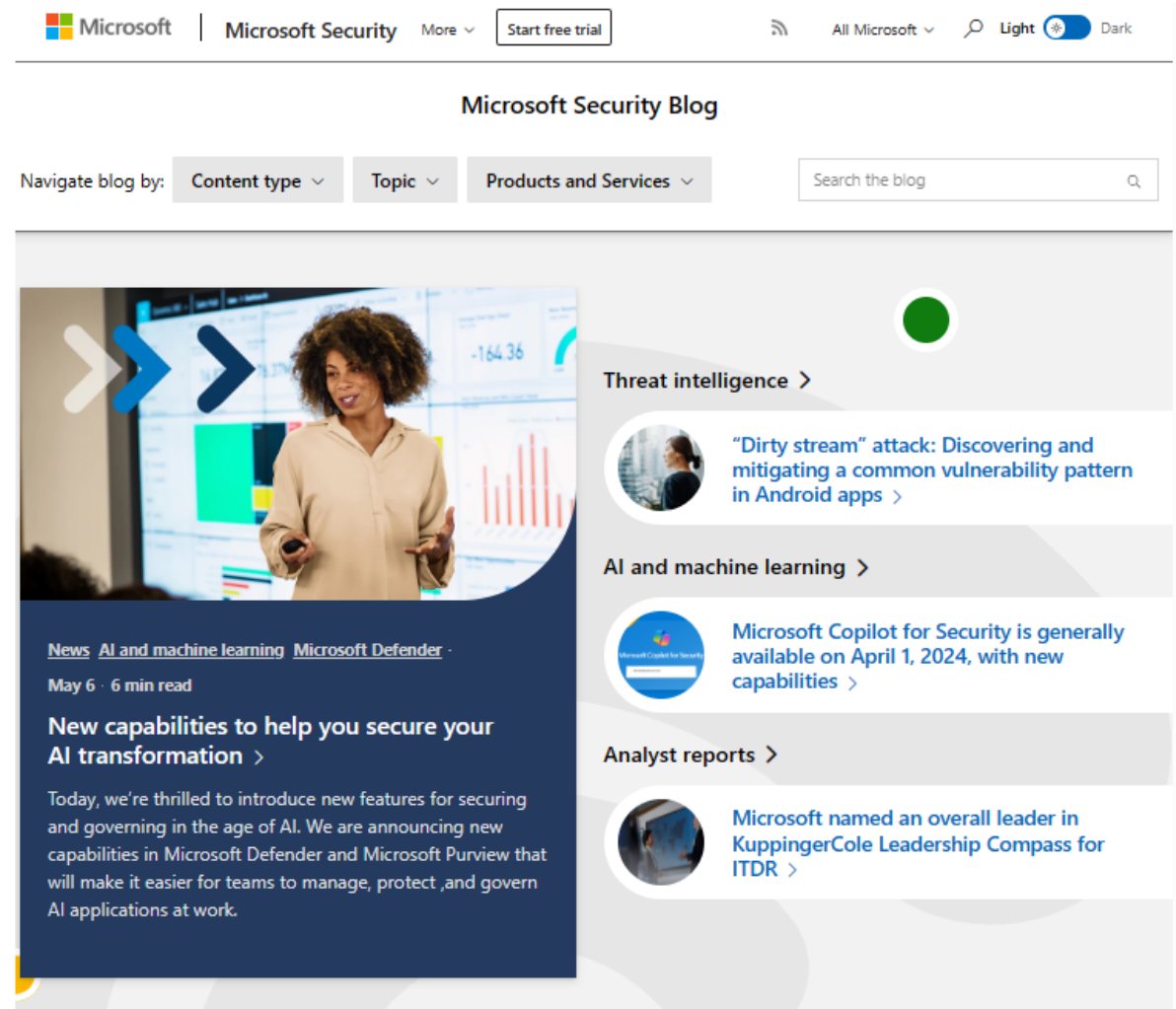
Publications by Microsoft Security

Microsoft Security Blog

[Microsoft Security Blog](#) is a valuable resource for staying informed about digital security, threat intelligence, and best practices.

Here are some highlights of the content you can find there:

1. **Best Practices:** The blog covers the latest best practices to keep you informed about what's happening in digital security.
2. **Threat Intelligence:** Expert coverage on security matters, including insights into emerging threats, vulnerabilities, and attack patterns.
3. **Product Updates and Announcements:** The blog provides information about new capabilities, security updates, and product releases.



2. Tracking Known Issues

Tracking Known Issues Caused by Security Updates

- Known issues are documented on the KB articles of each security updates.
- Notifications: If you want to keep eyes on known issues and issue status, please utilize below
 - [Description of Software Update Services and Windows Server Update Services changes in content for 2024 \(KB894199\) - Microsoft Support](#)
 - [Feed Picker - Microsoft Support](#)
 - [\[M365\] Windows known issue email alerts](#)

[M365] Windows known issue email alerts

- You can get notified about Windows known issues documented in the [Windows release health](#) section of the Microsoft 365 admin center.
- This enables you to easily and quickly learn about issues related to Windows updates and make informed decisions about rolling out an update across your environment.
- When you sign up, you'll receive emails about new issues for the versions of the Windows operating system you support, as well as updates to known issues such as:
 - Changes in issue status
 - New workarounds
 - Issue resolution
- This new feature is available to IT admins with a Windows or Microsoft 365 tenant, a subscription that provides access to Windows release health in the Microsoft 365 admin center^[1], and an eligible admin role.
- Read more at: <https://aka.ms/WRH/NotifyMe>



Watch this short video for a quick step-by-step on how to set up email notifications for Windows known issues.

<https://yQSD7fYyodC4outu.be/>

3. Tracking Security Enforcements in upcoming Security Updates

Tracking Security Enforcements in upcoming Security Updates

- Some security fix requires a functionality change that might impact system compatibility.
- For such security fix, Microsoft takes “Phased Rollout” to avoid compatibility issues.
- Example phased rollout schedule
 - Initial phase: release security updates that contains security fix. Fix is OFF by default. Users need to enable security fix by changing a registry value.
 - Second phase: release security updates to enable security fix by default. Users still can disable security fix by changing a registry value.
 - Enforcement phase: release security updates to enable security fix by default. Users are not disable security fix.
- Users need to review the security fix impact and enable security fix as soon as possible.

[Windows] Tracking Security Enforcements in upcoming Security Updates

- Please see the summary of Windows hardening guidance and key dates at: [Latest Windows hardening guidance and key dates - Microsoft Community Hub](#)
- Please bookmark the [Windows message center](#) to easily find the latest updates and reminders. And if you are an IT admin with access to the Microsoft 365 admin center, set up [Email preferences on the Microsoft 365 admin center](#) to receive important notifications and updates.

4. Tracking Product Lifecycle information

Microsoft Lifecycle Policy

- Microsoft provides industry-leading lifecycle policies - in length and provision - giving customers consistent, transparent, and predictable guidelines for software support and servicing.
- Please make sure to use products that are in product support lifecycle to receive security updates.
- [Fixed Lifecycle Policy](#) - products with defined end-of-support dates at the time of release.
- [Modern Lifecycle Policy](#) - products with continuous support and servicing.
- To view a comprehensive list of Microsoft product lifecycles, including migration options, please visit the [Microsoft Product Lifecycle Search](#) page.
- For information about service packs, see the [Fixed Lifecycle Policy](#). To see a list of commonly asked questions and answers on our policies and the Extended Security Update (ESU) program, please visit the following resources:
 - [Fixed Policy FAQs](#)
 - [Modern Policy FAQs](#)
 - [Extended Security Update \(ESU\) FAQs](#)

Additional Resources for Premier/Unified Customers

Microsoft Monthly Security Briefing

Microsoft Security Response Center (MSRC) releases security updates on monthly basis that address security vulnerabilities in Microsoft software, describe their remediation, and provide links to the applicable updates for affected software.

This Security Briefing will provide concise, actionable information for IT professionals and security decision makers about the month's release. The session, hosted by Microsoft security subject matter experts, starts with a brief technical overview of the latest security bulletins and related content. The remainder of the session is dedicated to customer questions or concerns in an interactive, question-and-answer format.

- **Presenter:** Security team, Customer Services and Support
- **Dates:** Patch Tuesday week
- **Available Language:** English (US, EMEA, APAC), Spanish, Portuguese, Italian, Traditional Chinese, Simplified Chinese, Japanese, Korean
- **Target Audience:** This Security Briefing is targeting Chief Information Security Officers, Security Vulnerability Assessors, IT Admins, and other security software update deployment decision makers
- **Key Features and Benefits:**
 - Learn about this month's security bulletin release.
 - Consolidated information - security update information is typically scattered in a variety of sources.
 - Get your questions about the security updates and advisories answered.
 - Get current product lifecycle information.

Microsoft Monthly Security Briefing

How to subscribe invitation for Microsoft Monthly Security Briefing:

1. Sign in to [Services Hub](#)
2. Navigate to Upper right-hand corner and click your account name and click [My Profile]
3. Navigate to [Communications] and click [Edit]
4. Click [Filters] and type "Security Briefing" in [Name]
5. Change [Subscribed] to [Yes] for the security briefing call in your region/language.

Communications

Set your preferences for Services Hub email updates and newsletters

- ☐ I want to participate in Microsoft Enterprise Support research. I agree to these terms and conditions. [Terms & Conditions](#)
- ☒ I would like information, tips, and offers about Microsoft Enterprise Support, including the Services Hub. [Privacy Statement](#)

Newsletters

Select the toggle for newsletters you want to receive and save your choices.

Customer: Contoso Company

Subscription changes will be applied to: yurikam@microsoft.com

Newsletters Count (8)

[Clear Filters](#) [Hide Filters](#)

Name	Description	Frequency	Language	Subscribed
security briefing				All
Subscribed	Name	Language	Frequ...	Description
<input type="radio"/> No	Security Briefing AMS Call Invite - Portug...	Portuguese	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing APAC Call Invite - Japane...	Japanese	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing AMS Call Invite - Spanish	Spanish	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing AMS Call Invite - English	English	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing APAC Call Invite - Chinese	Chinese	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing APAC Call Invite - Korean	Korean	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input checked="" type="radio"/> Yes	Security Briefing APAC Call Invite - English	English	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security
<input type="radio"/> No	Security Briefing APAC Call Invite - Taiwan...	Chinese (Traditio...	Monthly	The event is designed to give our customers the latest, pertinent information surrounding the Security

Test Guidance for Microsoft Security Updates (TGMSU)

- Test Guidance for Microsoft Security Updates (TGMSU) is a guide designed for Microsoft partners and customers to test Microsoft monthly security updates specific to their own environment and priorities.
- Microsoft recommends that customers evaluate the security updates on a case-by-case basis and use the test scenarios to allow granular testing of features or functionalities that are critical to you and your business.
- No single document can include all customer scenarios or possible tests, nor can any set of tests discover or prevent all issues. As such, test scenarios are provided to help testers understand the functional behavior and do not comprise a comprehensive list of all recommended test measures.

