

OPSWAT.

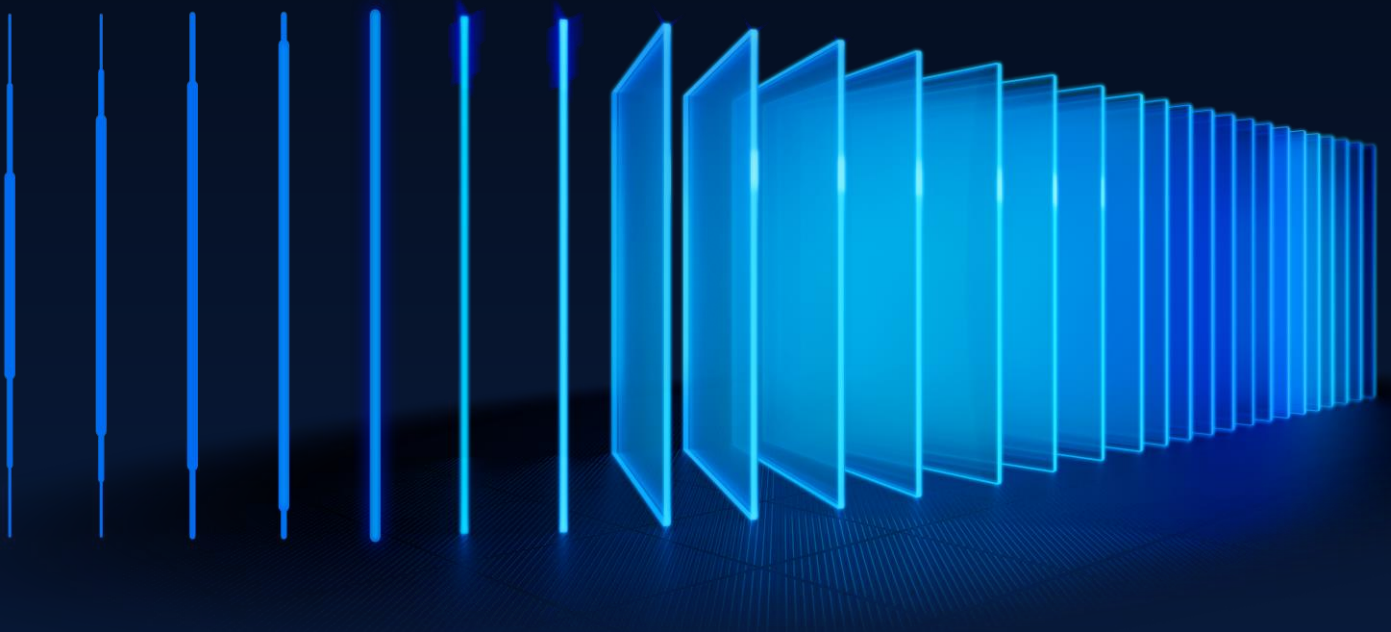
SDK News

OESIS Framework Update

February 2026

Announcement Date

2026/02/10



Contents

OESIS Framework Release Announcement February 2026	2
1 – What’s New?	3
1.1 New Software Categories for Compliance	3
1.2 The Mozilla Firefox patching behavior is changed on Windows.....	3
1.3 Removal of html5shiv for OESIS Documentation.....	4
1.4 New "usable_download_link" field in products.json	4
1.5 Introducing date_added timestamp for new patches	4
1.6 Support for the Windows 10 Extended Security Updates (ESU) program	4
1.7 Separating Zoom Signature for EXE and MSI Installers.....	5
2– Upcoming Changes	5
2.1 Improved Readability for raw_json.js in compliance.zip	6
2.2 Support for Patching Multiple App Instances on macOS	6
2.3 Notepad++ detection updates for Windows.....	6
2.4 Real-time monitoring on macOS	6
3 – Required Actions	7
3.1 February Release Schedule Update	8
3.2 Release Cadence Change (Starting April)	8
3.3 CVE-2025-0131	8
3.4 We moved the OesisPackageLinks.xml behind the VCR gateway	8
3.5 End of Support for AppRemover package with the old engine on macOS	9
3.6 End of Support for Windows 7 & Windows 8	9
4 – Detailed SDK Information	9
4.1 Windows Support Charts	10
4.2 Mac Support Charts.....	10
4.3 Linux Support Charts	10
4.4 SDK API Documentation	10
5 – Contact	10



OESIS Framework Release Announcement

February 2026

Please review the Required Actions in section 3 that you need to take soon.

1 – What's New?

We are thrilled to unveil the latest updates to the OESIS Framework this month. Get ready to supercharge your endpoint protection solutions with expanded support for more products and some new, exciting features. Build stronger defenses with advanced capabilities that integrate seamlessly into your products. Prepare for an epic upgrade that'll take your security to the next level.

1.1 New Software Categories for Compliance

NEW FEATURE, ALL PLATFORMS, ENGINE UPDATE NEEDED, CODE CHANGE

We are pleased to introduce three new software categories: Vulnerability Management, Artificial Intelligence, and Gaming.

All new categories include comprehensive support methods such as version detection, running state, installation directories, and more.

We've already added several products and will continue expanding these categories in the coming updates. Stay tuned!

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

1.2 The Mozilla Firefox patching behavior is changed on Windows

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

From January 13, 2026, the value of the "requires_reboot" parameter on server-side data, which could be used during the patching process, has changed from 0 (restart not required) to 2 (conditional restart).

In addition, when patching Mozilla Firefox using the InstallFromFiles method, the return codes will be as follows:

- **(Current)** If Mozilla Firefox does not require the application to restart after patching, the return code will be WA_API_OK (0).
- **(New)** If Mozilla Firefox does require the application to restart after patching, the return code will be WA_VMOD_INSTALLATION_NEED_APPLICATION_RESTART (1005).

This change reflects an update on Mozilla Firefox's patching behavior. An application restart is now required after patching to fully upgrade the application version. Without a restart, the patching process will not be completed, and the application version will remain unchanged.

1.3 Removal of html5shiv for OESIS Documentation

ENHANCEMENT, ANALOG PACKAGE

We have removed the legacy **html5shiv** from all SDK repositories across Windows, macOS, and Linux. This change is driven by application security considerations related to html5shiv and will impact only old browsers, specifically **Internet Explorer 6–9**, **Safari 4.x** (including iPhone 3.x), and **Firefox 3.x**. These browsers will no longer be able to correctly load OESIS documentation and support charts.

Modern browsers, including Microsoft Edge, have been fully validated: SDK and AR documentation and support charts continue to display and function properly.

1.4 New "usable_download_link" field in products.json

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

We have added a new "usable_download_link" boolean field to each product entry in analog/server/products.json. This field indicates whether the installer download link from GetLatestInstaller(download=0) is valid or not.

- If "usable_download_link" is true, agents will be able to use the download link.
- If "usable_download_link" is false, agents should not attempt to use it.

This update will help improve reliability by providing clear guidance to agents. To reduce failed download attempts, please plan to update your integration logic to check this field before fetching installer links.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

1.5 Introducing date_added timestamp for new patches

ENHANCEMENT, ANALOG PACKAGE, DATA UPDATE NEEDED, CODE CHANGE

Based on customer feedback, we've enhanced OESIS data so that all newly published patches now include a "date_added" timestamp in Analog patch metadata (specifically patch_aggregation.json).

This allows you to easily see when a specific patch first becomes available in our data.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

1.6 Support for the Windows 10 Extended Security Updates (ESU) program

ENHANCEMENT, WINDOWS, DATA UPDATE NEEDED

As of October 14, 2025, Microsoft no longer provides security patches, feature updates, or technical support for Windows 10. Windows 10 systems will still function, but become progressively vulnerable to security threats and software compatibility issues.

Therefore, Microsoft is introducing [the Windows 10 Extended Security Updates \(ESU\) program](#), which gives customers the option to receive security updates for PCs enrolled in the program.

To extend support for Windows 10 and ensure the Framework remains compatible with future updates of Windows 10, we have decided to continue supporting Windows 10 via [the Windows 10 Extended Security Updates \(ESU\) program](#). This support will be applied to devices running Windows 10, version 22H2 with [KB5046613](#), or a later update installed, and [having an active ESU subscription](#).

1.7 Separating Zoom Signature for EXE and MSI Installers

BEHAVIOR CHANGE, [WINDOWS](#), DATA UPDATE NEEDED

As part of this month's release, we have improved our Zoom detection on Windows by separating the existing Zoom signature into distinct entries for the MSI installer and the EXE package.

The previous Zoom signature (1872) is now dedicated to Zoom EXE, and a new signature has been added specifically for the Zoom MSI (ID: 4107). This change aligns with Zoom's end of support for x86 while ensuring that fresh installations and detections of Zoom on supported architectures continue to work reliably.

2– Upcoming Changes

2.1 Improved Readability for raw_json.js in compliance.zip

ENHANCEMENT, [ALL PLATFORMS](#), DATA UPDATE NEEDED

We will update the raw_json.js file in our Compliance data (for all platforms including Windows, macOS, Linux) to use a pretty-printed JSON format. This improves readability for customers who inspect or troubleshoot the data manually.

As a result, the Compliance package (compliance.zip) is slightly larger (from ~13 MB to ~14 MB), but no changes are required for existing integrations that programmatically consume this file.

2.2 Support for Patching Multiple App Instances on macOS

ENHANCEMENT, [MAC](#), ENGINE UPDATE NEEDED, [CODE CHANGE](#)

We are pleased to inform you that our team is actively investigating ways to improve patching support on macOS.

In the future release, our SDK will support patching multiple instances of applications, even when they are renamed or installed outside the standard Applications folder.

This enhancement ensures that after patching, only the latest version remains, eliminating unpatched or vulnerable duplicates across all locations.

2.3 Notepad++ detection updates for Windows

BEHAVIOR CHANGE, [WINDOWS](#), DATA UPDATE NEEDED

To improve Notepad++ coverage, we are splitting the existing detection signature **3241** (Notepad++) into three separate signatures: **x64 exe** (updated detection logic on the current signature 3241), **x64 msi** (new signature), and **arm64** (new signature).

After this change, some Notepad++ installations will no longer be detected under signature 3241 and will instead appear under the new signatures corresponding to their installer architecture.

2.4 Real-time monitoring on macOS

NEW FEATURE, MAC, ENGINE UPDATE NEEDED, CODE CHANGE

In Q1-2026, the SDK will provide **Real-time monitoring** on Mac operating systems. Unlike the current compliance checks, which are on-demand audits, real-time monitoring is dynamic, adapting to live events and rule changes as they occur.

More details will be provided in the coming months regarding which compliance statuses will be supported in this first phase.

Please note that this feature has been moved from Q4-2025 to Q1-2026.

You will need to make a code change to implement this feature. Please contact the OPSWAT team to assist with this

3 – Required Actions

3.1 February Release Schedule Update

RELEASE SCHEDULE UPDATE, [ALL PLATFORMS](#)

Our February Engine Package release schedule will be adjusted due to the Lunar New Year holiday. The planned releases on February 10, February 17, and February 24 will be skipped. The final release in February will take place on February 3, and our regular release cadence will resume after the holiday with the next release scheduled for March 3. We appreciate your understanding and wish you a happy Lunar New Year.

If you have any concerns or need clarification on this update, please contact the OPSWAT team to assist with this

3.2 Release Cadence Change (Starting April)

RELEASE SCHEDULE UPDATE, [ALL PLATFORMS](#)

Starting in April, we will be updating our Engine Package release cadence from weekly to bi-weekly. Under this new schedule, releases will occur twice per month, once in the second week and once in the fourth week of each month. This change aligns with our new development framework, enabling more accurate estimations, clearer updates, and more reliable on-time releases. We believe this adjustment will help us deliver higher-quality updates more consistently.

If you have any concerns or need clarification on this update, please contact the OPSWAT team to assist with this

3.3 CVE-2025-0131

VULNERABILITY, [WINDOWS](#)

An incorrect privilege management vulnerability in the OPSWAT OESIS Framework used by the Palo Alto Networks GlobalProtect™ app on Windows devices allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY\SYSTEM. However, execution requires that the local user also successfully exploits a race condition, which makes this vulnerability difficult to exploit.

To address CVE-2025-0131, please upgrade your Framework to version **4.3.4451** or later.

3.4 We moved the OesisPackageLinks.xml behind the VCR gateway

SECURITY UPDATE, [VCR GATEWAY](#)

Since **December 31st, 2024**, the OesisPackageLinks.xml file are relocated behind the VCR Gateway for enhanced security, replacing its currently public location.

Since September 1st, 2024, the file can be accessed via the VCR Gateway. You can download the file by following these steps: copy and paste this URL:



https://vcr.opswat.com/gw/file/download/OesisPackageLinks.xml?type=1&token=<authorization_token> in to your browser and replace **<authorization_token>** with your unique token. If you don't have a unique token, please [contact support](#).

This update ensures continued and secure access, and users should have updated their systems to accommodate this change.

3.5 End of Support for AppRemover package with the old engine on macOS

END OF SUPPORT, [MAC](#)

As we have refactored the AppRemover module on macOS to provide a more optimized and streamlined experience, two packages of the AppRemover module on macOS are being maintained on the My OPSWAT Portal: AppRemover OSX and AppRemover OSX V2.

Starting **January 1, 2026**, the OSX package will be removed. We recommend upgrading to AppRemover OSX V2 to ensure your system receives all new updates and comprehensive technical support for the AppRemover module.

3.6 End of Support for Windows 7 & Windows 8

END OF SUPPORT, [WINDOWS](#)

After careful consideration, support for Windows 7 and Windows 8 (server versions included) will be removed from the SDK beginning **January 1st 2027** (one year later than previous planned).

To ensure security, compatibility, and optimal performance with the OESIS Framework, we recommend upgrading endpoints to a supported Microsoft operating system.

4 – Detailed SDK Information

This is just the tip of the iceberg! You can view all the supported applications on our support charts:

4.1 [Windows Support Charts](#)

4.2 [Mac Support Charts](#)

4.3 [Linux Support Charts](#)

4.4 [SDK API Documentation](#)

5 – Contact

Are you a customer and have questions about this list? Please contact our trusted support team at opswat-support@opswat.com.

OPSWAT is a global leader in IT, OT, and ICS critical infrastructure cybersecurity, and for the last 20 years has continuously evolved an end-to-end solutions platform that empowers public and private sector organizations with the critical advantage needed to protect their complex networks and ensure compliance. OPSWAT solves customers' cybersecurity challenges around the world with zero-trust solutions and patented technologies across every level of their infrastructure, securing their networks, data, and devices, and preventing known and unknown threats, zero-day attacks, and malware.

For more information visit

www.opswat.com

OPSWAT.

Protecting the World's Critical Infrastructure

©2024 OPSWAT, Inc. All rights reserved. OPSWAT®, MetaDefender®, MetaAccess, Trust No File, Trust No Device, and the OPSWAT logo are trademarks of OPSWAT, Inc.