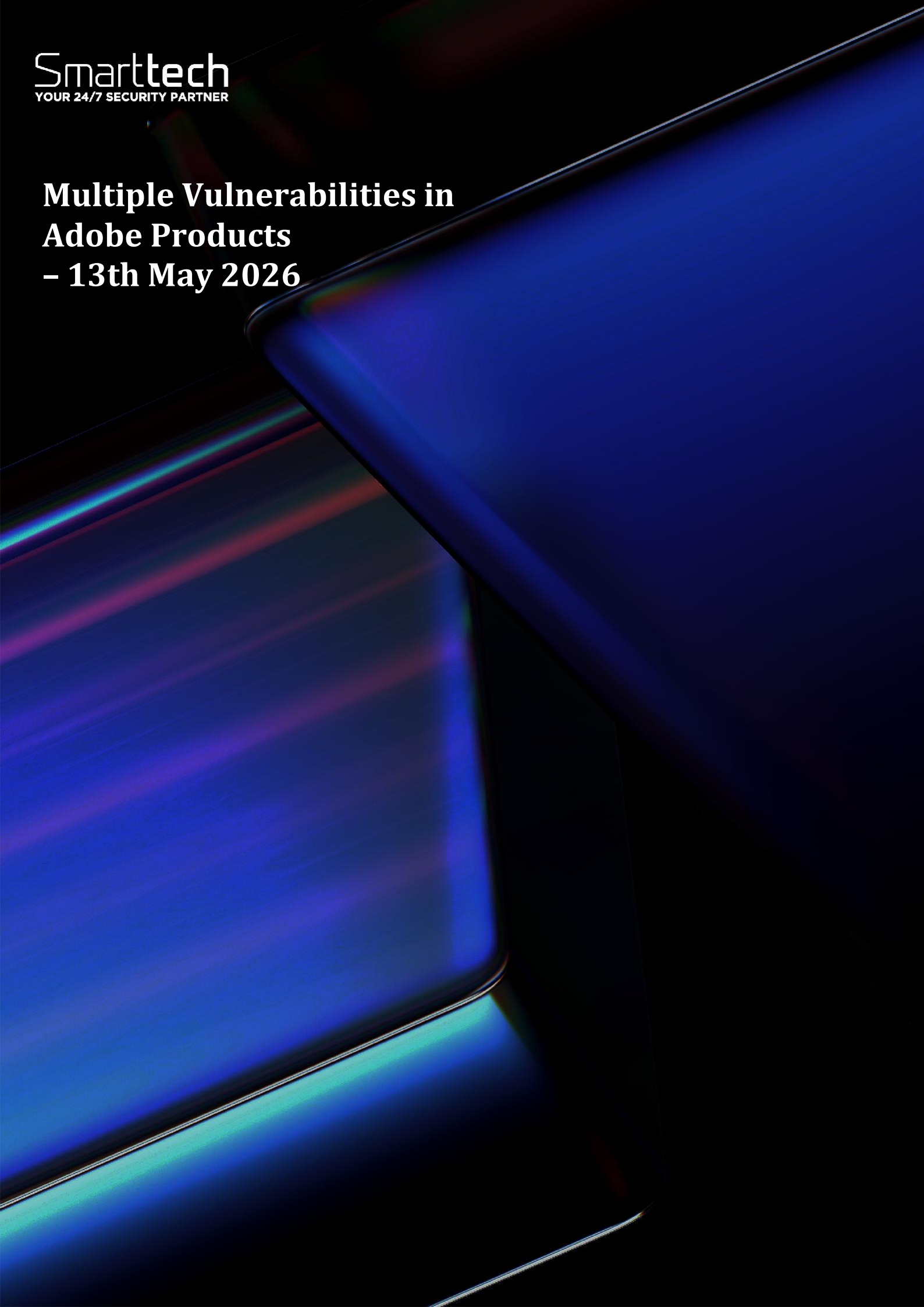
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Adobe Products – 13th May 2026



Document ID	SMA-Informative Cyber Alert
Document status	ISSUED
Authors	Daniel-Cristian Carp < daniel.carp@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	13th May 2026
Issue Date	12th May 2026

Informative Cyber Alerts are reports created by Smarttech247 designed to inform customers about medium and low severity vulnerabilities, IOCs from certain attacks/breaches, and other information that could help companies be aware and protect against any attack.
The content of this report should be regarded as simply informative as it usually addresses products that have an auto-update option available for patches. It will be the customer's decision if it is necessary to follow any recommendation or disregard them as they are not currently applicable in the environment.

Overview

Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user in question, an attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Technical Summary

Details of these vulnerabilities are as follows:

Tactic: Execution (TA0002)

Technique: Exploitation for Client Execution (T1203):

Adobe After Effects:
- Stack-based Buffer Overflow (CVE-2026-34641)
- Heap-based Buffer Overflow (CVE-2026-34642)
- Out-of-bounds Write (CVE-2026-34643)
- Integer Overflow or Wraparound (CVE-2026-34644)

Adobe Commerce:
- Incorrect Authorization (CVE-2026-34645, CVE-2026-34646)
- Server-Side Request Forgery (SSRF) (CVE-2026-34647)
- Uncontrolled Resource Consumption (CVE-2026-34648, CVE-2026-34649, CVE-2026-34650, CVE-2026-34651, CVE-2026-34652)
- Cross-site Scripting (Stored XSS) (CVE-2026-34686, CVE-2026-34655, CVE-2026-34658)
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CVE-2026-34653, CVE-2026-34654)
- Improper Authorization (CVE-2026-34656)
- Improper Input Validation (CVE-2026-34685)

Adobe Connect:
- Deserialization of Untrusted Data (CVE-2026-34659)
- Incorrect Authorization (CVE-2026-34660, CVE-2026-34659)

Adobe Media Encoder:
- Out-of-bounds Write (CVE-2026-34639)
- Integer Overflow or Wraparound (CVE-2026-34640)

Adobe Premiere Pro:
- Out-of-bounds Write (CVE-2026-34636, CVE-2026-34637)
- Use After Free (CVE-2026-34638)

Substance 3D Designer:
- Server-Side Request Forgery (SSRF) (CVE-2026-34664)

- Out-of-bounds Write (CVE-2026-34681, CVE-2026-34682, CVE-2026-34683, CVE-2026-34684)

Substance 3D Painter:
- Out-of-bounds Write (CVE-2026-34675, CVE-2026-34676)

Substance 3D Sampler:
- Heap-based Buffer Overflow (CVE-2026-34674)

Content Authenticity SDK:
- Uncontrolled Resource Consumption (CVE-2026-34665, CVE-2026-34673, CVE-2026-34677, CVE-2026-34678)
- Improper Input Validation (CVE-2026-34666, CVE-2026-34668, CVE-2026-34669, CVE-2026-34670, CVE-2026-34688, CVE-2026-34679)
- Integer Underflow (Wrap or Wraparound) (CVE-2026-34667, CVE-2026-34672)
- Integer Overflow or Wraparound (CVE-2026-34671, CVE-2026-34680)

Adobe Illustrator:
- Out-of-bounds Write (CVE-2026-34661)
- NULL Pointer Dereference (CVE-2026-34662)
- Out-of-bounds Read (CVE-2026-34663)
- Heap-based Buffer Overflow (CVE-2026-34687)

Affected Products

Adobe After Effects:

Product	Affected Versions	Platform
Adobe After Effects	25.6.4 and earlier versions	Windows and macOS
Adobe After Effects	26.0 and earlier versions	Windows and macOS

Adobe Commerce:

Product	Affected version	Platform
Adobe Commerce	2.4.4-p17 and earlier versions	Windows and macOS
Adobe Commerce	2.4.5-p16 and earlier versions	Windows and macOS
Adobe Commerce	2.4.6-p14 and earlier versions	Windows and macOS
Adobe Commerce	2.4.7-p9 and earlier versions	Windows and macOS
Adobe Commerce	2.4.8-p4 and earlier versions	Windows and macOS
Adobe Commerce	2.4.9-beta1	Windows and macOS
Adobe Commerce B2B	1.3.3-p17 and earlier versions	Windows and macOS
Adobe Commerce B2B	1.3.4-p16 and earlier versions	Windows and macOS

Adobe Commerce B2B	1.4.2-p9 and earlier versions	Windows and macOS
Adobe Commerce B2B	1.5.2-p4 and earlier versions	Windows and macOS
Adobe Commerce B2B	1.5.3-beta1	Windows and macOS

Adobe Connect Desktop Application:

Product	Affected version	Platform
Adobe Connect Desktop Application	2026.3.125	Windows
Adobe Connect Desktop Application	2026.01.39	macOS

Adobe Media Encoder:

Product	Affected version	Platform
Adobe Media Encoder	25.6.4 and earlier versions	Windows and macOS
Adobe Media Encoder	26.0.2 and earlier versions	Windows and macOS

Adobe Premiere:

Product	Affected version	Platform
Adobe Premiere	26.0.2 and earlier versions	Windows and macOS
Adobe Premiere Pro	25.6.4 and earlier versions	Windows and macOS

Adobe Substance 3D:

Product	Affected version	Platform
Adobe Substance 3D Designer	15.1.0 and earlier versions	Windows and macOS
Adobe Substance 3D Painter	12.0.2 and earlier versions	Windows and macOS
Adobe Substance 3D Sampler	5.1.3 and earlier versions	Windows and macOS

Content Authenticity:

Product	Affected version	Platform
Content Authenticity JS SDK	@contentauth/c2pa-web@0.7.1	Windows and macOS
Content Authenticity Rust SDK	c2pa-v0.80.1	Windows and macOS

Illustrator:

Product	Affected version	Platform
Illustrator 2025	29.8.6 and earlier versions	Windows and macOS
Illustrator 2026	30.3 and earlier versions	Windows and macOS

Magento Open Source:

Product	Affected version	Platform
Magento Open Source	2.4.6-p14 and earlier versions	Windows and macOS
Magento Open Source	2.4.7-p9 and earlier versions	Windows and macOS
Magento Open Source	2.4.8-p4 and earlier versions	Windows and macOS
Magento Open Source	2.4.9-beta1	Windows and macOS

Recommendations

Smarttech247 team recommends the following actions to be taken:

- Apply the stable channel update provided by Adobe to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct

application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 2.3: Address Unauthorized Software:** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
    - **Safeguard 2.7: Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file

types attempting to enter the enterprise's email gateway.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. **(M1050: Exploit Protection)**
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft? Data Execution Prevention (DEP), Windows? Defender Exploit Guard (WDEG), or Apple? System Integrity Protection (SIP) and Gatekeeper™.
- Block execution of code on a system through application control, and/or script blocking. (**M1038: Execution Prevention**)
    - **Safeguard 2.5: Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6: Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7: Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040: Behavior Prevention on Endpoint**)
    - **Safeguard 13.2: Deploy a Host-Based Intrusion Detection Solution:** Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7: Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

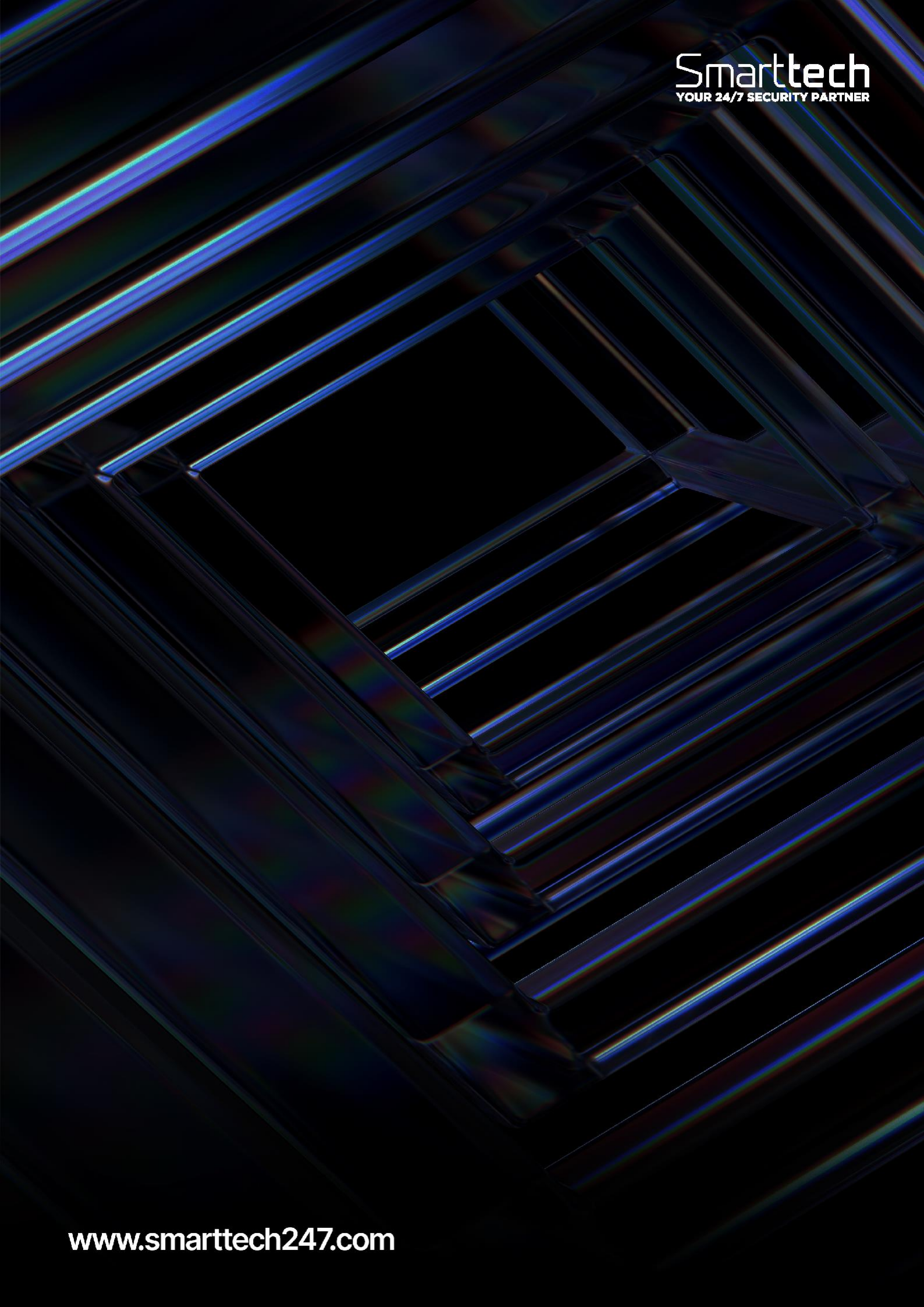
References

https://helpx.adobe.com/security/Home.html
https://helpx.adobe.com/security/products/premiere_pro/apsb26-46.html
https://helpx.adobe.com/security/products/media-encoder/apsb26-47.html
https://helpx.adobe.com/security/products/after_effects/apsb26-48.html
https://helpx.adobe.com/security/products/magento/apsb26-49.html
https://helpx.adobe.com/security/products/connect/apsb26-50.html
https://helpx.adobe.com/security/products/illustrator/apsb26-51.html
https://helpx.adobe.com/security/products/substance3d_designer/apsb26-52.html
https://helpx.adobe.com/security/products/content-authenticity-sdk/apsb26-53.html
https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-54.html
https://helpx.adobe.com/security/products/substance3d_painter/apsb26-55.html
https://helpx.adobe.com/security/Home.html

CVEs

CVE-2026-34636
CVE-2026-34637
CVE-2026-34638
CVE-2026-34639
CVE-2026-34640
CVE-2026-34641
CVE-2026-34642
CVE-2026-34643
CVE-2026-34644
CVE-2026-34645
CVE-2026-34646
CVE-2026-34647
CVE-2026-34648
CVE-2026-34649
CVE-2026-34650
CVE-2026-34651
CVE-2026-34652
CVE-2026-34653
CVE-2026-34654
CVE-2026-34655
CVE-2026-34656
CVE-2026-34658
CVE-2026-34659
CVE-2026-34660
CVE-2026-34661
CVE-2026-34662
CVE-2026-34663
CVE-2026-34664
CVE-2026-34665
CVE-2026-34666
CVE-2026-34667
CVE-2026-34668
CVE-2026-34669
CVE-2026-34670
CVE-2026-34671
CVE-2026-34672
CVE-2026-34673
CVE-2026-34674
CVE-2026-34675
CVE-2026-34676
CVE-2026-34677
CVE-2026-34678

CVE-2026-34679
CVE-2026-34680
CVE-2026-34681
CVE-2026-34682
CVE-2026-34683
CVE-2026-34684
CVE-2026-34685
CVE-2026-34686
CVE-2026-34687
CVE-2026-34688


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com