Coordinated Security & Privacy Disclosure, Final Report

Microsoft Edge for Android (com.microsoft.emmx)

An undisclosed employer remote-wipe capability over a personal browser, three portal redirects, zero data-protection answers

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, THREE PORTAL REDIRECTS, ZERO DATA-PROTECTION ANSWERS

Target	Microsoft Corporation (EU establishment referenced as Microsoft Ireland Operations Ltd.)
Product audited	Microsoft Edge for Android, com.microsoft.emmx, v149.0.4022.67
Disclosure reference	REF MSEDGE-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Intune MAM undisclosed remote-wipe capability, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Microsoft Edge Android application and identified five findings, two CRITICAL, three HIGH. The most significant: the Microsoft Intune MAM SDK, 583 smali classes, activates when a work or school account tied to an Intune-managed Azure AD tenant is signed into Edge on a personal device, granting the employer's IT department remote wipe of Edge's local browsing history, saved passwords, cookies, bookmarks, and downloaded files, copy-paste restrictions, and compliance telemetry logging, with no in-app notification that signing in with a work account activates this employer management.

Separately, the Adjust advertising-attribution SDK is embedded in a browser with no processor disclosure, and Microsoft's own 1DS telemetry pipeline transmits RequiredDiagnosticData that cannot be disabled by the user at all, alongside OptionalDiagnosticData defaulted to on. Two further findings concern Microsoft Copilot AI transmitting page context and conversation history to Azure AI without a confirmed explicit share action, and enterprise-grade data-loss-prevention and payment-processing components bundled into a consumer browser with no distinct disclosure.

Seven written notices were sent over 90 days. The only reply received was a single automated redirect to Microsoft's security bug-bounty portal, a channel for vulnerability submissions, not data-protection questions. RFI-IRFOS declined this redirect the same day. No further reply of any kind, from a human, a data-protection contact, or any other Microsoft address, was received through the close of the embargo.

Scope: Static analysis of the publicly downloaded production Microsoft Edge Android APK, on an authorized test device, only. No Microsoft account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to MSPrivacy@microsoft.com and secure@microsoft.com, bcc the Austrian DSB and CERT.at. MSPrivacy@microsoft.com bounced on every one of three delivery attempts. secure@microsoft.com produced one automated reply redirecting to the Microsoft Researcher Portal, a security-bug-bounty channel, not a data-protection contact. RFI-IRFOS declined the redirect in writing. No further reply of any kind was received across five subsequent written notices and 90 days.

ID	Severity	Title
C1	CRITICAL	Adjust SDK: advertising-attribution tracking embedded in a browser
C2	CRITICAL	Microsoft Intune MAM: undisclosed employer remote-wipe capability over personal browser data
H1	HIGH	1DS telemetry: non-disableable required diagnostics, pre-ticked optional diagnostics
H2	HIGH	Microsoft Copilot AI: page context and conversation transmission without a confirmed explicit share action

ID	Severity	Title
H3	HIGH	Enterprise DLP and payment processing bundled into a consumer browser

Subject & Operator Analysis

Microsoft Corporation operates Microsoft Edge for Android for a global consumer and enterprise user base, with Microsoft Ireland Operations Ltd. referenced as the relevant EU establishment and the Irish DPC as lead supervisory authority.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Adjust SDK: advertising-attribution tracking embedded in a browser

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

214 Adjust GmbH (Berlin) smali classes. On install, Adjust receives the device advertising ID and install referrer; session signals fire every time the browser opens, and custom conversion events fire for actions including onboarding completion, Copilot activation, and account sign-in.

No response was received naming this finding, including the direct question of Adjust's Art. 6(1) lawful basis and where it is named as a processor in the privacy notice.

Impact: Advertising-attribution tracking of browsing sessions and in-app conversion events operates with no confirmed processor disclosure.

Fix: Name Adjust GmbH as a data processor under Art. 13(1)(e) and publish the Art. 6(1) legal basis for advertising-attribution tracking in a browser context.

C2: Microsoft Intune MAM: undisclosed employer remote-wipe capability over personal browser data

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, 9.3

583 Microsoft Intune MAM smali classes activate when a work or school account tied to an Intune-managed Azure AD tenant is signed into Edge on a personal device.

No response was received naming this finding, including whether EU Edge users are informed at the point of work-account sign-in that this activates employer management. Once active, the employer's IT administrators gain: remote wipe of Edge's local data, browsing history, saved passwords, cookies, bookmarks, and downloaded files; copy-paste data-loss-prevention restrictions to non-managed apps; blocking of saved-file export to personal storage; conditional-access policy enforcement; and Intune diagnostic and compliance telemetry logging. No in-app notification informs the user that work-account sign-in has activated this employer-side management capability.

Impact: An employer can remotely wipe or restrict personal browser data on a personal device with no confirmed user-facing notification that this capability was activated.

Fix: Add an explicit, unavoidable in-app notice at the moment a work account activates Intune MAM management, disclosing the specific capabilities granted to the employer.

H1: 1DS telemetry: non-disableable required diagnostics, pre-ticked optional diagnostics

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

libtelclient.so, liboneds.so, and libctxlog.so transmit RequiredDiagnosticData and OptionalDiagnosticData to Microsoft's OneCollector endpoint. RequiredDiagnosticData cannot be disabled by the user under any setting found. OptionalDiagnosticData defaults to enabled.

No response was received naming this finding. A category of telemetry the user cannot disable forecloses the Art. 21 right to object by design, and a default-on optional category raises Art. 7 valid-consent questions.

Impact: A category of diagnostic telemetry cannot be disabled by the user under any available setting, and a second category defaults to collection without an opt-in action.

Fix: Provide a genuine opt-out for RequiredDiagnosticData or reclassify it, and default OptionalDiagnosticData to off pending explicit consent.

H2: Microsoft Copilot AI: page context and conversation transmission without a confirmed explicit share action

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

5,422 combined smali classes across Copilot's chat and edge-message-delegate components transmit conversation history and current-page context to Azure AI.

No response was received naming this finding. Copilot reportedly receives context from the current page without a confirmed explicit user share action, engaging Art. 22 automated-processing disclosure requirements.

Impact: Page content and conversation data may be transmitted to an AI processing backend without a confirmed explicit user action authorizing that specific transmission.

Fix: Confirm and disclose the specific trigger condition for page-context transmission to Copilot, and require an explicit user action for any transmission beyond the active chat input.

H3: Enterprise DLP and payment processing bundled into a consumer browser

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

Microsoft Information Protection (enterprise content-classification DLP) and com.microsoft.xpay (payment card data processing) are both bundled into the consumer browser binary.

No response was received naming this finding.

Impact: Enterprise data-loss-prevention and payment-processing components operate within a consumer product with no distinct Art. 13 disclosure or confirmed PCI-DSS notice.

Fix: Disclose both components' presence and function under Art. 13, and confirm applicable PCI-DSS scope for xpay.

Microsoft's Response, Recorded in Full

On 23 July 2026, secure@microsoft.com replied, in full: "Microsoft is no longer accepting new submissions through secure@microsoft.com. Please use the Microsoft Researcher Portal to report all potential product or service security vulnerabilities. For more information, or if you are unable to use the Researcher Portal, please visit our FAQs. Thank you for contacting the Microsoft Security Response Center and for your partnership in protecting customers."

This is the only reply received in the entire case. It redirects to a security vulnerability bug-bounty channel, not a data-protection contact, and does not address any of the five findings. RFI-IRFOS declined the redirect the same day, stating this is a GDPR data-protection disclosure, not a vulnerability submission. MSPrivacy@microsoft.com, the actual data-protection intake address named in R1, bounced on every one of three delivery attempts across the entire correspondence and was never reached. No further reply of any kind followed.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(e), Art. 5(1)(c), Art. 6(1)(a)	Undisclosed ad-attribution processor in a browser
C2	GDPR Art. 13(1), Art. 5(1)(f)	Undisclosed employer remote-wipe capability
H1	GDPR Art. 21, Art. 7	Non-disableable required telemetry, default-on optional telemetry
H2	GDPR Art. 22	Undisclosed AI page-context transmission trigger
H3	GDPR Art. 13	Undisclosed enterprise DLP and payment components

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to MSPrivacy@microsoft.com (bounces) and secure@microsoft.com, bcc Austrian DSB/CERT.at, 5 findings
2026-06-28	Follow-up #1, MSPrivacy@microsoft.com bounces again; embargo explicitly stated as 2026-09-19 for the first time
2026-07-23	secure@microsoft.com redirects to the Researcher Portal (bug-bounty channel); RFI-IRFOS declines same day, MSPrivacy bounces a third time
2026-08-15 / 08-24	Follow-ups restate all findings and three standing questions, Art. 33(4) 72-hour clock argument invoked
2026-09-04 / 09-12	Final follow-ups; deadline set then passed unanswered; weekly SHA-256 re-pull instituted
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Seven written notices across 90 days produced exactly one reply, an automated redirect to a security bug-bounty portal unrelated to data-protection questions. The actual data-protection intake address bounced on every attempt. All five findings, including an undisclosed employer remote-wipe capability, stand exactly as originally reported.

Residual Risk & Recommendations

- Add an explicit, unavoidable in-app notice disclosing employer management capabilities the moment a work account activates Intune MAM; this is the single highest-priority item given the confidentiality and integrity exposure to personal browser data.
- Name Adjust GmbH as a processor and publish its Art. 6(1) legal basis.
- Provide a genuine opt-out for RequiredDiagnosticData and default OptionalDiagnosticDa ta to off.
- Confirm and disclose Copilot's page-context transmission trigger condition.
- Repair the MSPrivacy@microsoft.com intake channel, confirmed bounced on every at- tempt across the entire case.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elis- abethinergasse 25/10, 8020 Graz, Austria