Security Bulletins for HUAWEI Phones/Tablets, April 2026

HUAWEI is releasing monthly security updates for flagship models. This security update includes HUAWEI and third-party library patches:

This security update includes the following HUAWEI patches:

CVE	Vulnerability Description	Impact	Severity	Affected Version
CVE-2026-28553	Vulnerability of improper permission control in the theme setting module	Successful exploitation of this vulnerability may affect service confidentiality.	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-34853	Permission bypass vulnerability in the LBS module	Successful exploitation of this vulnerability may affect availability.	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-34856	UAF vulnerability in the communication module	Successful exploitation of this vulnerability may affect availability.	High	HarmonyOS6.0.0

CVE-2026-34849	in the screen management module	this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34850	Race condition vulnerability in the notification service	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34851	Race condition vulnerability in the event notification module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34852	Stack overflow vulnerability in the media platform	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0
CVE-2026-34854	UAF vulnerability in the kernel module	Successful exploitation of this vulnerability will affect availability and confidentiality.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0, HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0

	Vulnerability			
CVE-2026-34855	Out-of-bounds write vulnerability in the kernel module	this vulnerability will affect availability and confidentiality.	Medium	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-34857	UAF vulnerability in the communication module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34858	UAF vulnerability in the communication module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34859	UAF vulnerability in the kernel module	Successful exploitation of this vulnerability will affect availability and confidentiality.	Medium	HarmonyOS4.3.0, HarmonyOS4.2.0, EMUI 15.0.0, EMUI 14.2.0
CVE-2026-34860	Access control vulnerability in the memo module	Successful exploitation of this vulnerability will affect availability	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0

Vulnerability				
CVE-2026-34861	Race condition vulnerability in the thermal management module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0
CVE-2026-34862	Race condition vulnerability in the power consumption statistics module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0
CVE-2026-34863	Out-of-bounds write vulnerability in the file system	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-34864	Boundary-unlimited vulnerability in the application read module	Successful exploitation of this vulnerability may affect availability.	Medium	HarmonyOS6.0.0
CVE-2026-28549	Race condition vulnerability in the permission management service	Successful exploitation of this vulnerability may affect	Medium	HarmonyOS5.1.0

CVE-2026-34867	vulnerability in the multi-mode input system	this vulnerability may affect availability.	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0

This security update includes the following third-party library patches:

CVE	Severity	Affected Version
CVE-2024-43766	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48567	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48578	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48579	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.0.0, EMUI

CVE	Severity	Affected Version
CVE-2025-48582	High	HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48619	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48645	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-48646	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-0012	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0

CVE	Severity	Affected Version
		HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-0015	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-0025	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-0026	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, HarmonyOS3.1.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0, EMUI 13.0.0
CVE-2026-0035	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-47396	High	HarmonyOS4.0.0, EMUI 14.0.0

CVE	Severity	Affected Version
CVE-2025-47398	High	HarmonyOS4.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-59600	High	HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2026-21385	High	HarmonyOS4.2.0, HarmonyOS4.0.0, EMUI 14.2.0, EMUI 14.0.0
CVE-2025-38618	High	HarmonyOS4.0.0, HarmonyOS3.1.0, EMUI 14.0.0, EMUI 13.0.0
CVE-2025-48621	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, HarmonyOS3.1.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0, EMUI 13.0.0
CVE-2025-48639	High	HarmonyOS4.3.1, HarmonyOS4.3.0, HarmonyOS4.2.0, HarmonyOS4.0.0, HarmonyOS3.1.0, EMUI 15.0.0, EMUI 14.2.0, EMUI 14.0.0, EMUI 13.0.0
CVE-2025-9230	High	HarmonyOS6.0.0, HarmonyOS5.1.0

CVE	Severity	Affected Version
CVE-2026-25646	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-0990	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-1757	Medium	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-0989	Low	HarmonyOS6.0.0, HarmonyOS5.1.0
CVE-2026-0992	Low	HarmonyOS6.0.0, HarmonyOS5.1.0

Updated on: 2026-04-08

Accessories HUAWEI Music HiSuite [/en/support/hisuite/]

HUAWEI [/en/]

Smartphone[/en/phones/]Wearable[/en/wearables/]PC[/en/laptops/]Ta

Support[/en/support/]Community[/en/community/]

Celia [/en/emui/celia/]

HUAWEI Browser [/en/mobileservices/browser/]

HUAWEI Assistant TODAY [/en/mobileservices/assistant/]

Petal Maps [/en/mobileservices/petalmaps/]

HUAWEI Books [/en/mobileservices/books/]

HUAWEI Member Center [/en/mobileservices/member-center/]

HUAWEI Health [/en/mobileservices/health/]

HUAWEI AI Life [/en/mobileservices/ai-life/]

MeeTime [/en/mobileservices/meetime/]

ABOUT HUAWEI

About Us [/en/about-us/]

News [/en/press/news/]

Events [/en/press/events/]

Sustainability [/en/sustainability/]

Privacy [/en/privacy/]

Contact Us [/en/support/contact-us/]

Corporate [https://www.huawei.com/en/]

Enterprise [https://e.huawei.com/en/?ic_medium=hwdc&ic_source=cbg_header_ent]

Carrier [https://carrier.huawei.com/en/?ic_medium=hwdc&ic_source=cbg_header_car]

Join Us [https://career.huawei.com/reccampportal/campus4_index.html#campus4/content.html]

Connect With Us