



CVE-2017-2724

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-2724
State	PUBLIC
Assigner	psirt@huawei.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-22 19:29:00 UTC
Updated	2017-12-08 18:52:00 UTC
Description	Bastet in P10 Plus and P10 smart phones with software earlier than VKY-AL00C00B123 versions, earlier than VTR-AL00C

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	P10	-	All	All	All
Hardware	Huawei	P10	-	All	All	All
Operating System	Huawei	P10 Firmware	All	All	All	All
Operating System	Huawei	P10 Firmware	All	All	All	All
Hardware	Huawei	P10 Plus	-	All	All	All
Hardware	Huawei	P10 Plus	-	All	All	All
Operating System	Huawei	P10 Plus Firmware	All	All	All	All
Operating System	Huawei	P10 Plus Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Security Advisory - Multiple Buffer Overflow Vulnerabilities in Bastet of Huawei Smart Phone	CONFIRM	www.huawei.com	Vendor
Huawei Smart Phones Multiple Local Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	Third P
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)