



CVE-2017-6351

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

Summary

CVE	CVE-2017-6351
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-06 02:59:00 UTC
Updated	2017-09-01 01:29:00 UTC
Description	The WePresent WiPG-1500 device with firmware 1.0.3.7 has a manufacturer account that has a hardcoded username / pas

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Wepresent	Wipg-1500	-	All	All	All
Hardware	Wepresent	Wipg-1500	-	All	All	All
Operating System	Wepresent	Wipg-1500 Firmware	1.0.3.7	All	All	All
Operating System	Wepresent	Wipg-1500 Firmware	1.0.3.7	All	All	All

References

Reference	Source	Link
WePresent WiPG-1500 - Backdoor Account	EXPLOIT-DB	www.exploit-db.com
wePresent Wireless Presentation Systems	MISC	www.wepresentwifi.com
WePresent WiPG-1500 Device CVE-2017-6351 Hardcoded Password Security Bypass Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

Free CVE JSON API [cve.report/api](#)

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