



# CVE-2017-3216

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

## Summary

<b>CVE</b>	CVE-2017-3216
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-20 00:29:00 UTC
<b>Updated</b>	2019-10-09 23:27:00 UTC
<b>Description</b>	WiMAX routers based on the MediaTek SDK (libmtk) that use a custom httpd plugin are vulnerable to an authentication byp

## Risk And Classification

### Problem Types: CWE-306

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Greenpacket</a>	<a href="#">Ox350</a>	-	All	All	All
Hardware	<a href="#">Greenpacket</a>	<a href="#">Ox350</a>	-	All	All	All
Operating System	<a href="#">Greenpacket</a>	<a href="#">Ox350 Firmware</a>	-	All	All	All
Operating System	<a href="#">Greenpacket</a>	<a href="#">Ox350 Firmware</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Bm2022</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Bm2022</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Bm2022 Firmware</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Bm2022 Firmware</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-309m</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-309m</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-309m Firmware</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-309m Firmware</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-319m</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-319m</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-319m2w</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-319m2w</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-319m2w Firmware</a>	-	All	All	All

Operating System	<a href="#">Huawei</a>	<a href="#">Hes-319m2w Firmware</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-319m Firmware</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-319m Firmware</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-339m</a>	-	All	All	All
Hardware	<a href="#">Huawei</a>	<a href="#">Hes-339m</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-339m Firmware</a>	-	All	All	All
Operating System	<a href="#">Huawei</a>	<a href="#">Hes-339m Firmware</a>	-	All	All	All
Hardware	<a href="#">Mada</a>	<a href="#">Soho Wireless Router</a>	-	All	All	All
Hardware	<a href="#">Mada</a>	<a href="#">Soho Wireless Router</a>	-	All	All	All
Operating System	<a href="#">Mada</a>	<a href="#">Soho Wireless Router Firmware</a>	-	All	All	All
Operating System	<a href="#">Mada</a>	<a href="#">Soho Wireless Router Firmware</a>	-	All	All	All
Hardware	<a href="#">Zte</a>	<a href="#">Ox-330p</a>	-	All	All	All
Hardware	<a href="#">Zte</a>	<a href="#">Ox-330p</a>	-	All	All	All
Operating System	<a href="#">Zte</a>	<a href="#">Ox-330p Firmware</a>	-	All	All	All
Operating System	<a href="#">Zte</a>	<a href="#">Ox-330p Firmware</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218m</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218m</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218m1w</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218m1w</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218m1w Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218m1w Firmware</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218mw</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max218mw</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218mw Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218mw Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218m Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max218m Firmware</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max308m</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max308m</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max308m Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max308m Firmware</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max318m</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max318m</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max318m Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max318m Firmware</a>	-	All	All	All

Hardware	<a href="#">Zyxel</a>	<a href="#">Max338m</a>	-	All	All	All
Hardware	<a href="#">Zyxel</a>	<a href="#">Max338m</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max338m Firmware</a>	-	All	All	All
Operating System	<a href="#">Zyxel</a>	<a href="#">Max338m Firmware</a>	-	All	All	All

## References

Reference	Source	Link
404 - Page not found! - SEC Consult	MISC	<a href="#">blog.sec-cons</a>
Vulnerability Lab - SEC Consult	MISC	<a href="#">sec-consult.cc</a>
VU#350135 - Various WiMAX routers contain a authentication bypass vulnerability in custom libmtk httpd plugin	CERT-VN	<a href="#">www.kb.cert.o</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#)