



# CVE-2017-8838

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-8838
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-05 14:29:00 UTC
<b>Updated</b>	2017-08-13 01:29:00 UTC
<b>Description</b>	XSS via syncid exists on Peplink Balance 305, 380, 580, 710, 1350, and 2500 devices with firmware before fw-b305hw2_38

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Peplink</a>	<a href="#">1350hw2 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">1350hw2 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">2500 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">2500 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">380hw6 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">380hw6 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">580hw2 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">580hw2 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">710hw3 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">710hw3 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">B305hw2 Firmware</a>	7.0.1	All	All	All
Operating System	<a href="#">Peplink</a>	<a href="#">B305hw2 Firmware</a>	7.0.1	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 1350</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 1350</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 2500</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 2500</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 305</a>	-	All	All	All

Hardware	<a href="#">Peplink</a>	<a href="#">Balance 305</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 380</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 380</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 580</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 580</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 710</a>	-	All	All	All
Hardware	<a href="#">Peplink</a>	<a href="#">Balance 710</a>	-	All	All	All

## References

Reference	Source	Link
Bugtraq: X41-2017-005 - Multiple Vulnerabilities in peplink balance routers	MISC	<a href="https://seclists.org">seclists.org</a>
Peplink Balance Routers 7.0.0-build1904 - SQL Injection / Cross-Site Scripting / Information Disclosure	EXPLOIT-DB	<a href="https://www.exploit-db.com">www.exploit-db.com</a>
Advisory X41-2017-005: Multiple Vulnerabilities in Peplink Balance Routers   X41 D-SEC GmbH	MISC	<a href="https://www.x41-dsec.de">www.x41-dsec.de</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">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](https://status.cve.report)