



CVE-2013-0230

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-0230
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-01-31 21:55:00 UTC
Updated	2016-12-08 03:02:00 UTC
Description	Stack-based buffer overflow in the ExecuteSoapAction function in the SOAPAction handler in the HTTP service in MiniUPnP

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miniupnp Project	Miniupnpd	1.0	All	All	All
Application	Miniupnp Project	Miniupnpd	1.0	All	All	All

References

Reference	Source	Link
Information Security: Security Flaws in Univers... SecurityStreet	MISC	co
community.rapid7.com/servlet/servlet.FileDownload	MISC	co
community.rapid7.com/servlet/JiveServlet/download/2150-1-16596/SecurityFlawsUPnP.pdf	MISC	co
MiniUPnPd 1.0 (MIPS) - Remote Stack Overflow Remote Code Execution for AirTies RT Series - Multiple remote Exploit	EXPLOIT-DB	ww
MiniUPnP CVE-2013-0230 Stack-Based Buffer Overflow Vulnerabilities	BID	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

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](#)