

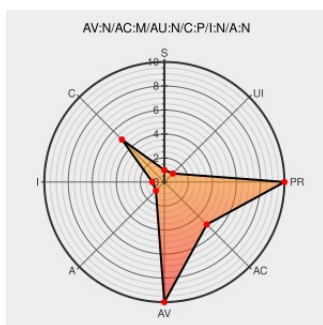


CVE-2014-9596

Published on: 01/15/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:00 PM UTC

CVE-2014-9596

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Arbitrator Back-end Server Mk 2.0 Vpu](#) from [Panasonic](#) contain the following vulnerability:

Panasonic Arbitrator Back-End Server (BES) MK 2.0 VPU before 9.3.1 build 4.08.003.0, when USB Wi-Fi or Direct LAN is enabled, and MK 3.0 VPU before 9.3.1 build 5.06.000.0, when Embedded Wi-Fi or Direct LAN is enabled, does not use encryption, which allows remote attackers to obtain sensitive information by sniffing the network for client-server traffic, as demonstrated by Active Directory credential information.

CVE-2014-9596 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

[Vendor Advisory](#)
[us2.campaign-archive1.com](#)
[text/plain](#)

[CONFIRM us2.campaign-archive1.com/?u=8c9cff2e712e3b7d09a07ecef&id=21f059b3ab](https://us2.campaign-archive1.com/?u=8c9cff2e712e3b7d09a07ecef&id=21f059b3ab)

Vulnerability Note VU#117604 - Panasonic Arbitrator Back-End Server (BES) uses unencrypted communication

[Third Party Advisory](#)
[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#117604](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Panasonic	Arbitrator Back-end Server Mk 2.0 Vpu	-	All	All	All
Hardware 	Panasonic	Arbitrator Back-end Server Mk 2.0 Vpu	-	All	All	All
Operating System	Panasonic	Arbitrator Back-end Server Mk 2.0 Vpu Firmware	All	All	All	All
Hardware 	Panasonic	Arbitrator Back-end Server Mk 3.0 Vpu	-	All	All	All
Hardware 	Panasonic	Arbitrator Back-end Server Mk 3.0 Vpu	-	All	All	All
Operating System	Panasonic	Arbitrator Back-end Server Mk 3.0 Vpu Firmware	All	All	All	All
cpe:2.3:h:panasonic:arbitrator_back-end_server_mk_2.0_vpu:-:*****:						
cpe:2.3:h:panasonic:arbitrator_back-end_server_mk_2.0_vpu:-:*****:						
cpe:2.3:o:panasonic:arbitrator_back-end_server_mk_2.0_vpu_firmware:*****:						
cpe:2.3:h:panasonic:arbitrator_back-end_server_mk_3.0_vpu:-:*****:						
cpe:2.3:h:panasonic:arbitrator_back-end_server_mk_3.0_vpu:-:*****:						
cpe:2.3:o:panasonic:arbitrator_back-end_server_mk_3.0_vpu_firmware:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→