



CVE-2004-0334

Published on: 03/18/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0334

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

Certain versions of [Innomedia Videophone](#) from [Innomedia](#) contain the following vulnerability:

InnoMedia VideoPhone allows remote attackers to bypass Basic Authorization via an HTTP request to (1) videophone_admindetail.asp, (2) videophone_syscfg.asp, (3) videophone_upgrade.asp, or (4) videophone_sysctrl.asp that contains a trailing / (slash). NOTE: the original report mentioned AXIS 2100 Network Camera, but this was likely a cut-and-paste error.

CVE-2004-0334 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

'InnoMedia VideoPhone Authorization Bypass' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040227 InnoMedia VideoPhone Authorization Bypass](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF InnoMedia-videophone-bypass-authentication\(15636\)](#)

SecurityTracker.com Archives - InnoMedia VideoPhone Lets Remote Users Bypass Authentication

[securitytracker.com](#)
[text/html](#)

[SECTrack 1009522](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 4809](#)

Inactive Link **Not Archived**

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

By selecting these links, you may be leaving CVEreport's website. We have provided these links to other resources 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 comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Innomedia	Innomedia Videophone	au75200xvi04010x	All	All	All
Hardware 	Innomedia	Innomedia Videophone	au75200xvi04010x	All	All	All
cpe:2.3:h:innomedia:innomedia_videophone:au75200xvi04010x:*****:						
cpe:2.3:h:innomedia:innomedia_videophone:au75200xvi04010x:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)