



CVE-2012-1805

Published on: 04/13/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:19 PM UTC

CVE-2012-1805

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 



Certain versions of [H0-ecom](#) from [Koyo](#) contain the following vulnerability:

Buffer overflow in the ECOM Ethernet module in Koyo H0-ECOM, H0-ECOM100, H2-ECOM, H2-ECOM-F, H2-ECOM100, H4-ECOM, H4-ECOM-F, and H4-ECOM100 allows remote attackers to execute arbitrary code via long strings in unspecified parameters.

CVE-2012-1805 has been assigned by  cert@cert.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

404 - File Not Found | CISA

[US Government Resource](#)
[www.us-cert.gov](#)
[application/pdf](#)
Inactive Link **Not Archived**

 MISC [www.us-cert.gov/control_systems/pdf/ICSA-12-102-02.pdf](#)

IBM X-Force Exchange

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

 XF [koyo-ecom-bo\(74875\)](#)

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 [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
Application	Koyo	H0-ecom	All	All	All	All
Application	Koyo	H0-ecom	All	All	All	All
Application	Koyo	H0-ecom100	All	All	All	All
Application	Koyo	H0-ecom100	All	All	All	All
Application	Koyo	H2-ecom	All	All	All	All
Application	Koyo	H2-ecom	All	All	All	All
Application	Koyo	H2-ecom-f	All	All	All	All
Application	Koyo	H2-ecom-f	All	All	All	All
Application	Koyo	H2-ecom100	All	All	All	All
Application	Koyo	H2-ecom100	All	All	All	All
Application	Koyo	H4-ecom	All	All	All	All
Application	Koyo	H4-ecom	All	All	All	All
Application	Koyo	H4-ecom-f	All	All	All	All
Application	Koyo	H4-ecom-f	All	All	All	All
Application	Koyo	H4-ecom100	All	All	All	All
Application	Koyo	H4-ecom100	All	All	All	All
cpe:2.3:a:koyo:h0-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h0-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h0-ecom100:*:*:*:*:*:						
cpe:2.3:a:koyo:h0-ecom100:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom-f:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom-f:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom100:*:*:*:*:*:						
cpe:2.3:a:koyo:h2-ecom100:*:*:*:*:*:						
cpe:2.3:a:koyo:h4-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h4-ecom:*:*:*:*:*:						
cpe:2.3:a:koyo:h4-ecom-f:*:*:*:*:*:						

cpe:2.3:a:koyo:h4-ecom-f:*****:
cpe:2.3:a:koyo:h4-ecom100:*****:
cpe:2.3:a:koyo:h4-ecom100:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→