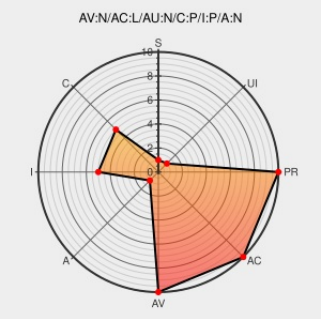
CVE-2004-2184

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2184

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Yak from Digicraft Software contain the following vulnerability:

Directory traversal vulnerability in Digicraft Yak! server 2.0 through 2.1.2 allows remote attackers to read or write arbitrary files via "../" or "..\" sequences in commands such as (1) dir or (2) put.

CVE-2004-2184 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF yak-directory-traversal(17740)
SecurityTracker.com Archives - Yak! Chat Directory Travesal Flaw Lets Remote Users Upload Files to Arbitrary Locations	securitytracker.com text/html	SECTRACK 1011708
'[Full-Disclosure] Directory traversal in Yak! 2.1.2' - MARC	marc.info text/html	FULLDISC 20041015 Directory traversal in Yak! 2.1.2
SecurityFocus	Exploit www.securityfocus.com text/html	BUGTRAQ 20041015 Directory traversal in Yak! 2.1.2
	Exploit aluigi.altervista.org text/plain	MISC aluigi.altervista.org/adv/yak-adv.txt

Yak! Chat Client FTP Server Directory Traversal Vulnerability	Exploit cve.report (archive) text/html	BID 11433
Secunia - Advisories - Yak! File Upload Directory Traversal Vulnerability	web.archive.org text/html	SECUNIA 12849
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 10763

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	Digicraft Software	Yak	2.0	All	All	All
Application	Digicraft Software	Yak	2.0.1	All	All	All
Application	Digicraft Software	Yak	2.0.2	All	All	All
Application	Digicraft Software	Yak	2.1.0	All	All	All
Application	Digicraft Software	Yak	2.1.1	All	All	All
Application	Digicraft Software	Yak	2.1.2	All	All	All
Application	Digicraft Software	Yak	2.0	All	All	All
Application	Digicraft Software	Yak	2.0.1	All	All	All
Application	Digicraft Software	Yak	2.0.2	All	All	All
Application	Digicraft Software	Yak	2.1.0	All	All	All
Application	Digicraft Software	Yak	2.1.1	All	All	All
Application	Digicraft Software	Yak	2.1.2	All	All	All

cpe:2.3:a:digicraft_software:yak:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:digicraft_software:yak:2.1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→