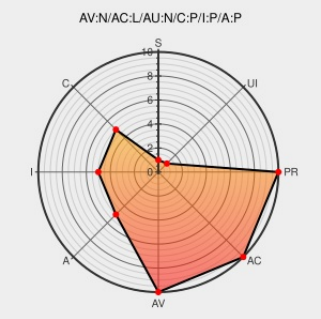
CVE-2004-2061

Published on: 07/27/2004 04:00:00 AM UTC

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

CVE-2004-2061

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



Certain versions of Risearch from Risearch Software contain the following vulnerability:

RiSearch 1.0.01 and RiSearch Pro 3.2.06 allows remote attackers to use the show.pl script as an open proxy, or read arbitrary local files, by setting the url parameter to a (1) http://, (2) ftp://, or (3) file:// URL.

CVE-2004-2061 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 8266
SecurityTracker.com Archives - RiSearch/Ri Search Pro Discloses Files to Remote Users and Can Be Used as an Open Proxy	securitytracker.com text/html	SECTRACK 1010788
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 8265
Secunia - Advisories - RiSearch Open Proxy Relay Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 12173
RiSearch/RiSearch Pro Open Proxy Vulnerability	Exploit	BID 10812

	Vendor Advisory cve.report (archive) text/html	
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF risearch-show-open-proxy(16817)
'IRM 009: RiSearch and RiSearch ProPro are vulnerable to open FTP/HTTP proxy, directory listings and' - MARC	marc.info text/html	BUGTRAQ 20040727 IRM 009: RiSearch and RiSearch ProPro are vulnerable to open FTP/HTTP proxy, directory listings and file disclosure vulnerabilities

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Risearch Software	Risearch	0.99.1	All	All	All
Application	Risearch Software	Risearch	0.99.2	All	All	All
Application	Risearch Software	Risearch	0.99.3	All	All	All
Application	Risearch Software	Risearch	0.99.4	All	All	All
Application	Risearch Software	Risearch	0.99.5	All	All	All
Application	Risearch Software	Risearch	0.99.6	All	All	All
Application	Risearch Software	Risearch	0.99.7	All	All	All
Application	Risearch Software	Risearch	0.99.8	All	All	All
Application	Risearch Software	Risearch	0.99.1	All	All	All
Application	Risearch Software	Risearch	0.99.2	All	All	All
Application	Risearch Software	Risearch	0.99.3	All	All	All
Application	Risearch Software	Risearch	0.99.4	All	All	All
Application	Risearch Software	Risearch	0.99.5	All	All	All
Application	Risearch Software	Risearch	0.99.6	All	All	All
Application	Risearch Software	Risearch	0.99.7	All	All	All
Application	Risearch Software	Risearch	0.99.8	All	All	All
Application	Risearch Software	Risearch Pro	3.2.6	All	All	All
Application	Risearch Software	Risearch Pro	3.2.6	All	All	All

cpe:2.3:a:risearch_software:risearch:0.99.1:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.2:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.3:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.4:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.5:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.6:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.7:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.8:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.1:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.2:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.3:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.4:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.5:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.6:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.7:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch:0.99.8:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch_pro:3.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:risearch_software:risearch_pro:3.2.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→