



Published on: 04/20/2004 04:00:00 AM UTC

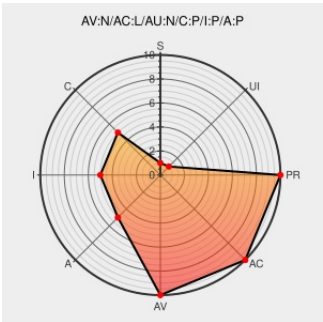
Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1945

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Exchange Pop3](#) from [Kinesphere Corporation](#) contain the following vulnerability:

Buffer overflow in Kinesphere eXchange POP3 allows remote attackers to execute arbitrary code via a long MAIL FROM field.

CVE-2004-1945 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
Kinesphere Corporation Exchange POP3 Remote Buffer Overflow Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	 BID 10180
'Re: Exchange pop3 remote exploit' - MARC	marc.info text/html	 BUGTRAQ 20040527 Re: Exchange pop3 remote exploit
'Exchange pop3 remote exploit' - MARC	marc.info text/html	 BUGTRAQ 20040419 Exchange pop3 remote exploit
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF exchange-pop3-smtp-bo(15922)

Secunia - Advisories - Kinesphere eXchange POP3 Buffer Overflow Vulnerability

Exploit

Patch

Vendor Advisory

web.archive.org

text/html

SECUNIA 11449

No Description Provided

www.osvdb.org

OSVDB 5593

Inactive Link

Not Archived

SecurityTracker.com Archives - eXchange POP3 Server SMTP Buffer Overflow Lets Remote Users Execute Arbitrary Code

Exploit

Vendor Advisory

securitytracker.com

text/html

SECTRAK 1009882

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	Kinesphere Corporation	Exchange Pop3	4.0	All	All	All
Application	Kinesphere Corporation	Exchange Pop3	5.0	All	All	All
Application	Kinesphere Corporation	Exchange Pop3	4.0	All	All	All
Application	Kinesphere Corporation	Exchange Pop3	5.0	All	All	All
cpe:2.3:a:kinesphere_corporation:exchange_pop3:4.0:*:*:*:*:*:						
cpe:2.3:a:kinesphere_corporation:exchange_pop3:5.0:*:*:*:*:*:						
cpe:2.3:a:kinesphere_corporation:exchange_pop3:4.0:*:*:*:*:*:						
cpe:2.3:a:kinesphere_corporation:exchange_pop3:5.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)