



CVE-2004-0121

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2004-0121
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-04-15 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Argument injection vulnerability in Microsoft Outlook 2002 does not sufficiently filter parameters of mailto: URLs when using

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-88 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Office	xp	sp2	All	All

Application	Microsoft	Outlook	2002	sp2	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	N/a	affected n/a		Not specified	
References						
Reference			Source			
marc.info			af854a3a-2127-422b-91ae-364			
iDEFENSE			af854a3a-2127-422b-91ae-364			
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364			
Repository / Oval Repository			af854a3a-2127-422b-91ae-364			
VU#305206 - Microsoft Outlook fails to properly filter parameters passed via "mailto:" URL			af854a3a-2127-422b-91ae-364			
www.ciac.org/ciac/bulletins/o-096.shtml			af854a3a-2127-422b-91ae-364			
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364			
Microsoft Security Bulletin MS04-009 - Critical Microsoft Docs			af854a3a-2127-422b-91ae-364			
US-CERT Technical Cyber Security Alert TA04-070A -- Microsoft Outlook mailto URL Handling Vulnerability			af854a3a-2127-422b-91ae-364			
Microsoft Outlook Mailto Parameter Quoting Zone Bypass Vulnerability			af854a3a-2127-422b-91ae-364			
CVE Program record			CVE.ORG			
NVD vulnerability detail			NVD			
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						