



CVE-2004-1936

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2004-1936
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-04-14 04:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	ZoneAlarm Pro 4.5.538.001 and possibly other versions allows remote attackers to bypass e-mail protection via attachment

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zonelabs	Zonealarm	2.4	All	pro	All
Application	Zonelabs	Zonealarm	2.6	All	pro	All
Application	Zonelabs	Zonealarm	3.0	All	pro	All
Application	Zonelabs	Zonealarm	3.1	All	pro	All
Application	Zonelabs	Zonealarm	4.0	All	plus	All
Application	Zonelabs	Zonealarm	4.0	All	pro	All
Application	Zonelabs	Zonealarm	4.5	All	pro	All
Application	Zonelabs	Zonealarm	4.5.538.001	All	plus	All
Application	Zonelabs	Zonealarm	4.5.538.001	All	pro	All
Application	Zonelabs	Zonealarm	2.4	All	pro	All
Application	Zonelabs	Zonealarm	2.6	All	pro	All
Application	Zonelabs	Zonealarm	3.0	All	pro	All
Application	Zonelabs	Zonealarm	3.1	All	pro	All
Application	Zonelabs	Zonealarm	4.0	All	plus	All
Application	Zonelabs	Zonealarm	4.0	All	pro	All
Application	Zonelabs	Zonealarm	4.5	All	pro	All
Application	Zonelabs	Zonealarm	4.5.538.001	All	plus	All

Application	Zonelabs	Zonealarm	4.5.538.001	All	pro	All
-------------	--------------------------	---------------------------	-------------	-----	-----	-----

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
ZoneLabs ZoneAlarm Pro/Plus MailSafe Filter Bypass Vulnerability	BID	www.securityfocus.com	
20040420 Re: ZA Security Hole	BUGTRAQ	marc.info	
20040414 ZA Security Hole	BUGTRAQ	marc.info	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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