



CVE-2008-3068

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2008-3068
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-07 23:41:00 UTC
Updated	2018-10-11 20:45:00 UTC
Description	Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Access	2007	All	All	All
Application	Microsoft	Access	2007	All	All	All
Application	Microsoft	Excel	2003	All	All	All
Application	Microsoft	Excel	2007	All	All	All
Application	Microsoft	Excel	2003	All	All	All
Application	Microsoft	Excel	2007	All	All	All
Application	Microsoft	Frontpage	2003	All	All	All
Application	Microsoft	Frontpage	2003	All	All	All
Application	Microsoft	Groove	2007	All	All	All
Application	Microsoft	Groove	2007	All	All	All
Application	Microsoft	Infopath	2003	All	All	All
Application	Microsoft	Infopath	2007	All	All	All
Application	Microsoft	Infopath	2003	All	All	All
Application	Microsoft	Infopath	2007	All	All	All
Application	Microsoft	Office	2007	All	All	All
Application	Microsoft	Office	2007	sp1	All	All
Application	Microsoft	Office	2007	All	All	All

Application	Microsoft	Office	2007	sp1	All	All
Application	Microsoft	Office Communicator	2007	All	All	All
Application	Microsoft	Office Communicator	2007	All	All	All
Application	Microsoft	Onenote	2003	All	All	All
Application	Microsoft	Onenote	2003	All	All	All
Application	Microsoft	Outlook	2003	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Microsoft	Outlook	2003	All	All	All
Application	Microsoft	Outlook	2007	All	All	All
Application	Microsoft	Powerpoint	2003	All	All	All
Application	Microsoft	Powerpoint	2007	All	All	All
Application	Microsoft	Powerpoint	2003	All	All	All
Application	Microsoft	Powerpoint	2007	All	All	All
Application	Microsoft	Project Professional	2007	All	All	All
Application	Microsoft	Project Professional	2007	All	All	All
Application	Microsoft	Project Standard	2007	All	All	All
Application	Microsoft	Project Standard	2007	All	All	All
Application	Microsoft	Publisher	2003	All	All	All
Application	Microsoft	Publisher	2007	All	All	All
Application	Microsoft	Publisher	2003	All	All	All
Application	Microsoft	Publisher	2007	All	All	All
Application	Microsoft	Sharepoint Designer	2007	All	All	All
Application	Microsoft	Sharepoint Designer	2007	All	All	All
Application	Microsoft	Visio Professional	2007	All	All	All
Application	Microsoft	Visio Professional	2007	All	All	All
Application	Microsoft	Visio Standard	2007	All	All	All
Application	Microsoft	Visio Standard	2007	All	All	All
Application	Microsoft	Windows Live Mail	2008	All	All	All
Application	Microsoft	Windows Live Mail	2008	All	All	All

References

Reference	Source	Link
CXSecurity - IDS	SREASON	securityreason.com
www.cynops.de/advisories/AKLINK-SA-2008-004.txt	MISC	www.cynops.de
www.cynops.de/techzone/http_over_x509.html	MISC	www.cynops.de

www.cynops.de/advisories/AKLINK-SA-2008-003.txt	MISC	www.cynops.de
SecurityFocus	BUGTRAQ	www.securityfocus.com
Microsoft Crypto API X.509 Certificate Validation Remote Information Disclosure Vulnerability	BID	www.securityfocus.com
Windows Live Mail S/MIME Processing Lets Remote Users Access Arbitrary URLs - SecurityTracker	SECTRACK	www.securitytracker.co
404 Not Found	MISC	www.klink.name
Microsoft Outlook S/MIME Processing Lets Remote Users Access Arbitrary URLs - SecurityTracker	SECTRACK	www.securitytracker.co
Microsoft Office S/MIME Processing Lets Remote Users Access Arbitrary URLs - SecurityTracker	SECTRACK	www.securitytracker.co
404 Not Found	MISC	www.klink.name
404 Not Found	MISC	www.klink.name
SecurityFocus	BUGTRAQ	www.securityfocus.com
www.cynops.de/advisories/AKLINK-SA-2008-002.txt	MISC	www.cynops.de
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org/cve). This site includes MITRE data granted under the following [license](http://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report