E-Mail Header Information Results

Sender Information

Name: "Hayes, Allison"
Organisation: NOT FOUND

Sender Software

Software: Microsoft Outlook

Found usernames

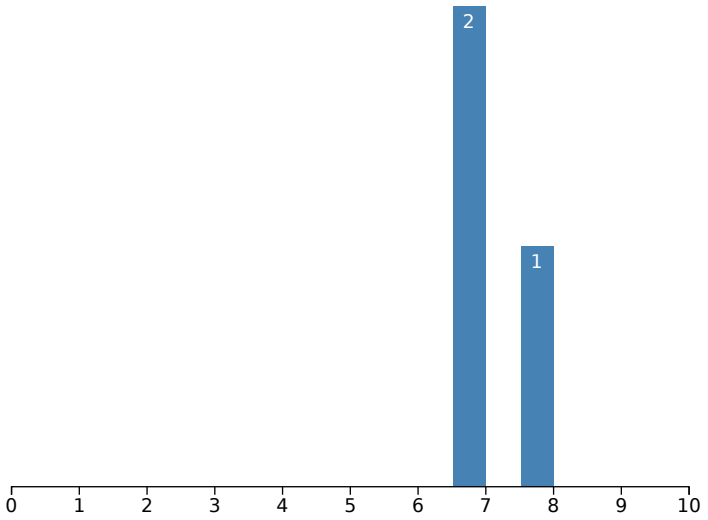
Class	Type	Details
Exchange	X-MS-Exchange-Organization-AVStamp-Mailbox	Sophos;-2052447998;0;PM
Exchange	X-MS-Exchange-Organization-AuthAs	Anonymous
Exchange	X-MS-Exchange-Organization-AuthSource	HUB01.ad.oak.ox.ac.uk
Exchange	X-MS-Exchange-Organization-SCL	2
Personal	Sender Information	"Hayes, Allison"
Application	Microsoft Outlook	Accept-Language

	Server	Time	Software	CVEs
0	163.1.154.218 (51.75,-1.25)		Microsoft SMTP Server	
1	129.67.1.163 (51.75,-1.25)		esmtp (Exim 4.80) (envelope-from)	

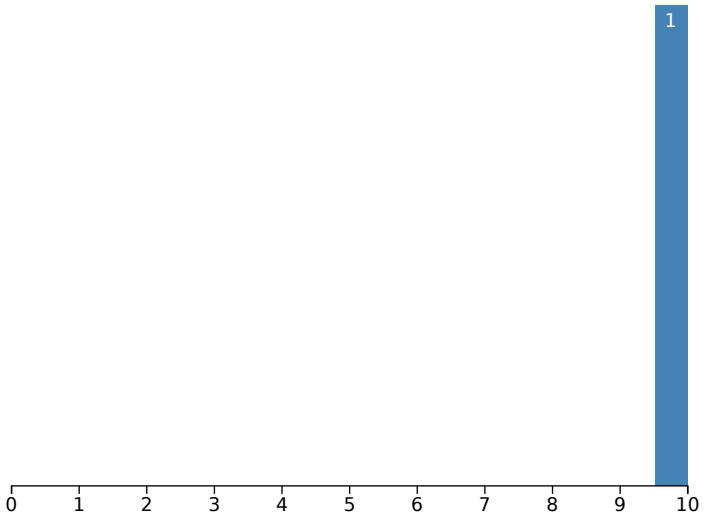
2	129.67.151.44 (51.75,-1.25)		esmtp (Exim 4.72) (envelope-from)	
3	129.67.151.81 (51.75,-1.25)		esmtp (Exim 4.72) (envelope-from)	
4	129.67.1.162 (51.75,-1.25)		esmtp (Exim 4.80) (envelope-from)	
5	128.194.216.124 (30.6521,-96.341)		mapi	

Distribution of CVE Scores by Product

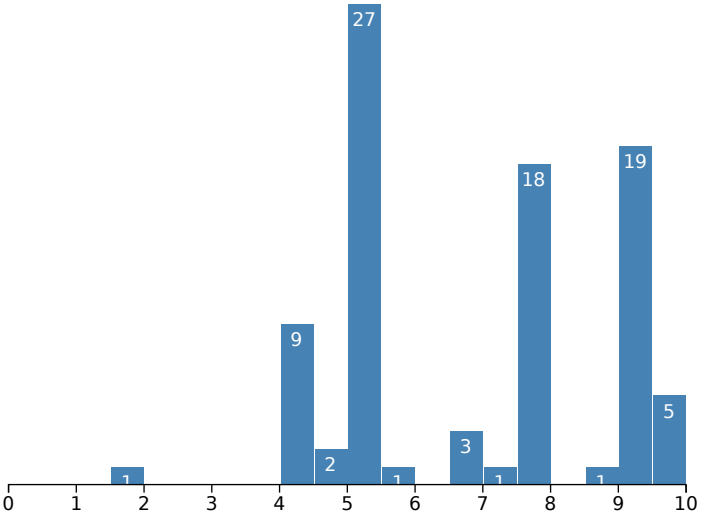
esmtp



mapi



outlook



Availability: Clear **Confidentiality:** Clear **Integrity:** Clear **Vector:** Clear **Complexity:** Clear
Authentication: Clear

Search

CVE-ID	Summary
CVE-2010-0266	Microsoft Office Outlook 2002 SP3, 2003 SP3, and 2007 SP1 and SP2 does not properly verify e-mail attachments with a PR_ATTACH_METHOD property value of ATTACH_BY_REFERENCE, which allows user-assisted remote attackers to execute arbitrary code via a crafted message, aka "Microsoft Outlook SMB Attachment Vulnerability."
CVE-2008-5424	The MimeOleClearDirtyTree function in InetComm.dll in Microsoft Outlook Express 6.00.2900.5512 does not properly handle (1) multipart/mixed e-mail messages with many MIME parts and possibly (2) e-mail messages with many "Content-type: message/rfc822;" headers, which allows remote attackers to cause a denial of service (infinite loop) via a large e-mail message, a related issue to CVE-2006-1173.
CVE-2002-1056	Microsoft Outlook 2000 and 2002, when configured to use Microsoft Word as the email editor, does not block scripts that are used while editing email messages in HTML or Rich Text Format (RTF), which could allow remote attackers to execute arbitrary scripts via an email that the user forwards or replies to.
CVE-2006-2057	Argument injection vulnerability in Mozilla Firefox 1.0.6 allows user-assisted remote attackers to modify command line arguments to an invoked mail client via " (double quote) characters in a mailto: scheme handler, as demonstrated by launching Microsoft Outlook with an arbitrary filename as an attachment. NOTE: it is not clear whether this issue is implementation-specific or a problem in the Microsoft API.
CVE-2007-2227	The MHTML protocol handler in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle Content-Disposition "notifications," which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka "Content Disposition Parsing Cross Domain Information Disclosure Vulnerability."
CVE-2005-1213	Stack-based buffer overflow in the news reader for Microsoft Outlook Express (MSOE.DLL) 5.5 SP2, 6, and 6 SP1 allows remote malicious NNTP servers to execute arbitrary code via a LIST response with a long second field.
CVE-2010-0816	Integer overflow in inetcomm.dll in Microsoft Outlook Express 5.5 SP2, 6, and 6 SP1; Windows Live Mail on Windows XP SP2 and SP3, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7; and Windows Mail on Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote e-mail servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) POP3 or (2) IMAP response, as demonstrated by a certain +OK response on TCP port 110, aka "Outlook Express and Windows Mail Integer Overflow Vulnerability."
CVE-2002-2100	Microsoft Outlook 2002 allows remote attackers to embed bypass the file download restrictions for attachments via an HTML email message that uses an IFRAME to reference malicious content.
CVE-1999-0519	A NETBIOS/SMB share password is the default, null, or missing.
CVE-2008-2143	Unspecified versions of Microsoft Outlook Web Access (OWA) use the Cache-Control: no-cache HTTP directive instead of no-store, which might cause web browsers that follow RFC-2616 to cache sensitive information.
CVE-2014-5359	Directory traversal vulnerability in SafeNet Authentication Service (SAS) Outlook Web Access Agent (formerly CRYPTOCard) before 1.03.30109 allows remote attackers to read arbitrary files via a .. (dot dot) in the GetFile parameter to owa/owa.
CVE-2008-4025	Integer overflow in Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via (1) an RTF file or (2) a rich text e-mail message containing an invalid number of points for a polyline or polygon, which triggers a heap-based buffer overflow, aka "Word RTF Object Parsing Vulnerability."
CVE-	Microsoft Outlook 2002 Connector for IBM Lotus Domino 2.0 allows local users to save passwords and login credentials locally, even

2005-0921	when password caching is disabled by a group policy.
CVE-2014-2510	The JAXB XML parser in EMC Documentum Foundation Services (DFS) 6.6 before P39, 6.7 SP1 before P28, and 6.7 SP2 before P15, as used in My Documentum for Desktop, My Documentum for Microsoft Outlook, and CenterStage, allows remote authenticated users to read arbitrary files via an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.
CVE-1999-0967	Buffer overflow in the HTML library used by Internet Explorer, Outlook Express, and Windows Explorer via the res: local resource protocol.
CVE-2008-4027	Double free vulnerability in Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; and Office 2004 for Mac allow remote attackers to execute arbitrary code via a crafted (1) RTF file or (2) rich text e-mail message with multiple consecutive Drawing Object ("\do") tags, which triggers a "memory calculation error" and memory corruption, aka "Word RTF Object Parsing Vulnerability."
CVE-2010-3147	Untrusted search path vulnerability in wab.exe 6.00.2900.5512 in Windows Address Book in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via a Trojan horse wab32res.dll file in the current working directory, as demonstrated by a directory that contains a Windows Address Book (WAB), VCF (aka vCard), or P7C file, aka "Insecure Library Loading Vulnerability." NOTE: the codebase for this product may overlap the codebase for the product referenced in CVE-2010-3143.
CVE-2000-0419	The Office 2000 UA ActiveX Control is marked as "safe for scripting," which allows remote attackers to conduct unauthorized activities via the "Show Me" function in Office Help, aka the "Office 2000 UA Control" vulnerability.
CVE-2007-4040	Argument injection vulnerability involving Microsoft Outlook and Outlook Express, when certain URIs are registered, allows remote attackers to conduct cross-browser scripting attacks and execute arbitrary commands via shell metacharacters in an unspecified URI, which are inserted into the command line when invoking the handling process, a similar issue to CVE-2007-3670.
CVE-2000-0567	Buffer overflow in Microsoft Outlook and Outlook Express allows remote attackers to execute arbitrary commands via a long Date field in an email header, aka the "Malformed E-mail Header" vulnerability.
CVE-2008-3068	Microsoft Crypto API 5.131.2600.2180 through 6.0, as used in Outlook, Windows Live Mail, and Office 2007, performs Certificate Revocation List (CRL) checks by using an arbitrary URL from a certificate embedded in a (1) S/MIME e-mail message or (2) signed document, which allows remote attackers to obtain reading times and IP addresses of recipients, and port-scan results, via a crafted certificate with an Authority Information Access (AIA) extension.
CVE-2008-4026	Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a crafted Word document that contains a malformed value, which triggers memory corruption, aka "Word Memory Corruption Vulnerability."
CVE-2006-2111	A component in Microsoft Outlook Express 6 allows remote attackers to bypass domain restrictions and obtain sensitive information via redirections with the mhtml: URI handler, as originally reported for Internet Explorer 6 and 7, aka "URL Redirect Cross Domain Information Disclosure Vulnerability."
CVE-2006-6659	The Microsoft Office Outlook Recipient ActiveX control (ole32.dll) in Windows XP SP2 allows remote attackers to cause a denial of service (Internet Explorer 7 hang) via crafted HTML.
CVE-2007-0034	Buffer overflow in the Advanced Search (Finder.exe) feature of Microsoft Outlook 2000, 2002, and 2003 allows user-assisted remote attackers to execute arbitrary code via a crafted Outlook Saved Searches (OSS) file that triggers memory corruption, aka "Microsoft Outlook Advanced Find Vulnerability."
CVE-2007-3897	Heap-based buffer overflow in Microsoft Outlook Express 6 and earlier, and Windows Mail for Vista, allows remote Network News Transfer Protocol (NNTP) servers to execute arbitrary code via long NNTP responses that trigger memory corruption.
CVE-2008-4024	Microsoft Office Word 2000 SP3 and 2002 SP3 and Office 2004 for Mac allow remote attackers to execute arbitrary code via a Word document with a crafted lcbPlcfBkfSdt field in the File Information Block (FIB), which bypasses an initialization step and triggers an "arbitrary free," aka "Word Memory Corruption Vulnerability."
CVE-1999-1033	Microsoft Outlook Express before 4.72.3612.1700 allows a malicious user to send a message that contains a .., which can inadvertently cause Outlook to re-enter POP3 command mode and cause the POP3 session to hang.
CVE-2005-4840	The Outlook Express Address Book control, when using Internet Explorer 6, allows remote attackers to cause a denial of service (NULL dereference and browser crash) by creating the OutlookExpress.AddressBook COM object, which is not intended for use within Internet Explorer.
CVE-2007-0671	Unspecified vulnerability in Microsoft Excel 2000, XP, 2003, and 2004 for Mac, and possibly other Office products, allows remote user-assisted attackers to execute arbitrary code via unknown attack vectors, as demonstrated by Exploit-MSExcel.h in targeted zero-day attacks.
CVE-2000-0653	Microsoft Outlook Express allows remote attackers to monitor a user's email by creating a persistent browser link to the Outlook Express windows, aka the "Persistent Mail-Browser Link" vulnerability.
CVE-2004-0121	Argument injection vulnerability in Microsoft Outlook 2002 does not sufficiently filter parameters of mailto: URLs when using them as arguments when calling OUTLOOK.EXE, which allows remote attackers to use script code in the Local Machine zone and execute arbitrary programs.

CVE-2001-0145	Buffer overflow in VCard handler in Outlook 2000 and 98, and Outlook Express 5.x, allows an attacker to execute arbitrary commands via a malformed vCard birthday field.
CVE-2014-5239	The Microsoft Outlook.com application before 7.8.2.12.49.7090 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2000-0415	Buffer overflow in Outlook Express 4.x allows attackers to cause a denial of service via a mail or news message that has a .jpg or .bmp attachment with a long file name.
CVE-2010-2728	Heap-based buffer overflow in Microsoft Outlook 2002 SP3, 2003 SP3, and 2007 SP2, when Online Mode for an Exchange Server is enabled, allows remote attackers to execute arbitrary code via a crafted e-mail message, aka "Heap Based Buffer Overflow in Outlook Vulnerability."
CVE-2006-0014	Buffer overflow in Microsoft Outlook Express 5.5 and 6 allows remote attackers to execute arbitrary code via a crafted Windows Address Book (WAB) file containing "certain Unicode strings" and modified length values.
CVE-2001-0322	MSHTML.DLL HTML parser in Internet Explorer 4.0, and other versions, allows remote attackers to cause a denial of service (application crash) via a script that creates and deletes an object that is associated with the browser window object.
CVE-2002-1179	Buffer overflow in the S/MIME Parsing capability in Microsoft Outlook Express 5.5 and 6.0 allows remote attackers to execute arbitrary code via a digitally signed email with a long "From" address, which triggers the overflow when the user views or previews the message.
CVE-2001-1547	Outlook Express 6.0, with "Do not allow attachments to be saved or opened that could potentially be a virus" enabled, does not block email attachments from forwarded messages, which could allow remote attackers to execute arbitrary code.
CVE-2003-0301	The IMAP Client for Outlook Express 6.00.2800.1106 allows remote malicious IMAP servers to cause a denial of service (crash) via certain large literal size values that cause either integer signedness errors or integer overflow errors.
CVE-2010-1568	The Send Secure functionality in the Cisco IronPort Desktop Flag Plug-in for Outlook before 6.5.0-006 does not properly handle simultaneously composed messages, which might allow remote attackers to obtain cleartext contents of e-mail messages that were intended to be encrypted, aka bug 65623.
CVE-2005-2226	Microsoft Outlook Express 6.0 leaks the default news server account when a user responds to a "watched" conversation thread, which could allow remote attackers to obtain sensitive information.
CVE-2002-0152	Buffer overflow in various Microsoft applications for Macintosh allows remote attackers to cause a denial of service (crash) or execute arbitrary code by invoking the file:// directive with a large number of / characters, which affects Internet Explorer 5.1, Outlook Express 5.0 through 5.0.2, Entourage v. X and 2001, PowerPoint v. X, 2001, and 98, and Excel v. X and 2001 for Macintosh.
CVE-2008-4837	Stack-based buffer overflow in Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; and Microsoft Works 8 allow remote attackers to execute arbitrary code via a crafted Word document that contains a malformed table property, which triggers memory corruption, aka "Word Memory Corruption Vulnerability."
CVE-2003-1048	Double free vulnerability in mshtml.dll for certain versions of Internet Explorer 6.x allows remote attackers to cause a denial of service (application crash) via a malformed GIF image.
CVE-2012-4328	Unspecified vulnerability in the MAPI in vBulletin Suite 4.1.2 through 4.1.12, Forum 4.1.2 through 4.1.12, and the MAPI plugin 1.4.3 for vBulletin 3.x has unknown impact and attack vectors.
CVE-2001-1325	Internet Explorer 5.0 and 5.5, and Outlook Express 5.0 and 5.5, allow remote attackers to execute scripts when Active Scripting is disabled by including the scripts in XML stylesheets (XSL) that are referenced using an IFRAME tag, possibly due to a vulnerability in Windows Scripting Host (WSH).
CVE-2000-0036	Outlook Express 5 for Macintosh downloads attachments to HTML mail without prompting the user, aka the "HTML Mail Attachment" vulnerability.
CVE-2004-0204	Directory traversal vulnerability in the web viewers for Business Objects Crystal Reports 9 and 10, and Crystal Enterprise 9 or 10, as used in Visual Studio .NET 2003 and Outlook 2003 with Business Contact Manager, Microsoft Business Solutions CRM 1.2, and other products, allows remote attackers to read and delete arbitrary files via ".." sequences in the dynamicimag argument to crystalimagehandler.aspx.
CVE-2012-1391	Unspecified vulnerability in the mOffice - Outlook sync (com.innov8tion.isharesync) application 3.1 for Android has unknown impact and attack vectors.
CVE-2002-0285	Outlook Express 5.5 and 6.0 on Windows treats a carriage return ("CR") in a message header as if it were a valid carriage return/line feed combination (CR/LF), which could allow remote attackers to bypass virus protection and or other filtering mechanisms via a mail message with headers that only contain the CR, which causes Outlook to create separate headers.
CVE-2008-4030	Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1 allow remote attackers to execute arbitrary code via crafted control words in (1) an RTF file or (2) a rich text e-mail message, which triggers incorrect memory allocation and memory corruption, aka "Word RTF Object Parsing Vulnerability," a different vulnerability than CVE-2008-4028.

CVE-2004-0284	Microsoft Internet Explorer 6.0, Outlook 2002, and Outlook 2003 allow remote attackers to cause a denial of service (CPU consumption), if "Do not save encrypted pages to disk" is disabled, via a web site or HTML e-mail that contains two null characters (%00) after the host name.
CVE-2004-0200	Buffer overflow in the JPEG (JPG) parsing engine in the Microsoft Graphic Device Interface Plus (GDI+) component, GDIPlus.dll, allows remote attackers to execute arbitrary code via a JPEG image with a small JPEG COM field length that is normalized to a large integer length before a memory copy operation.
CVE-2008-4031	Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a malformed string in (1) an RTF file or (2) a rich text e-mail message, which triggers incorrect memory allocation and memory corruption, aka "Word RTF Object Parsing Vulnerability."
CVE-2013-3870	Double free vulnerability in Microsoft Outlook 2007 SP3 and 2010 SP1 and SP2 allows remote attackers to execute arbitrary code by including many nested S/MIME certificates in an e-mail message, aka "Message Certificate Vulnerability."
CVE-2001-0538	Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page.
CVE-2000-0524	Microsoft Outlook and Outlook Express allow remote attackers to cause a denial of service by sending email messages with blank fields such as BCC, Reply-To, Return-Path, or From.
CVE-2006-4868	Stack-based buffer overflow in the Vector Graphics Rendering engine (vgx.dll), as used in Microsoft Outlook and Internet Explorer 6.0 on Windows XP SP2, and possibly other versions, allows remote attackers to execute arbitrary code via a Vector Markup Language (VML) file with a long fill parameter within a rect tag.
CVE-2003-0007	Microsoft Outlook 2002 does not properly handle requests to encrypt email messages with V1 Exchange Server Security certificates, which causes Outlook to send the email in plaintext, aka "Flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates could lead to Information Disclosure."
CVE-2004-0380	The MHTML protocol handler in Microsoft Outlook Express 5.5 SP2 through Outlook Express 6 SP1 allows remote attackers to bypass domain restrictions and execute arbitrary code, as demonstrated on Internet Explorer using script in a compiled help (CHM) file that references the InfoTech Storage (ITS) protocol handlers such as (1) ms-its, (2) ms-itss, (3) its, or (4) mk:@MSITStore, aka the "MHTML URL Processing Vulnerability."
CVE-2001-1088	Microsoft Outlook 8.5 and earlier, and Outlook Express 5 and earlier, with the "Automatically put people I reply to in my address book" option enabled, do not notify the user when the "Reply-To" address is different than the "From" address, which could allow an untrusted remote attacker to spoof legitimate addresses and intercept email from the client that is intended for another user.
CVE-2000-0105	Outlook Express 5.01 and Internet Explorer 5.01 allow remote attackers to view a user's email messages via a script that accesses a variable that references subsequent email messages that are read by the client.
CVE-2000-0160	The Microsoft Active Setup ActiveX component in Internet Explorer 4.x and 5.x allows a remote attacker to install software components without prompting the user by stating that the software's manufacturer is Microsoft.
CVE-2003-1378	Microsoft Outlook Express 6.0 and Outlook 2000, with the security zone set to Internet Zone, allows remote attackers to execute arbitrary programs via an HTML email with the CODEBASE parameter set to the program, a vulnerability similar to CAN-2002-0077.
CVE-2008-4028	Microsoft Office Word 2000 SP3, 2002 SP3, 2003 SP3, and 2007 Gold and SP1; Outlook 2007 Gold and SP1; Word Viewer 2003 Gold and SP3; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Gold and SP1; Office 2004 and 2008 for Mac; and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via crafted control words related to multiple Drawing Object tags in (1) an RTF file or (2) a rich text e-mail message, which triggers incorrect memory allocation and a heap-based buffer overflow, aka "Word RTF Object Parsing Vulnerability," a different vulnerability than CVE-2008-4030.
CVE-2006-2386	Unspecified vulnerability in Microsoft Outlook Express 6 and earlier allows remote attackers to execute arbitrary code via a crafted contact record in a Windows Address Book (WAB) file.
CVE-1999-0384	The Forms 2.0 ActiveX control (included with Visual Basic for Applications 5.0) can be used to read text from a user's clipboard when the user accesses documents with ActiveX content.
CVE-2000-0216	Microsoft email clients in Outlook, Exchange, and Windows Messaging automatically respond to Read Receipt and Delivery Receipt tags, which could allow an attacker to flood a mail system with responses by forging a Read Receipt request that is redirected to a large distribution list.
CVE-2000-0329	A Microsoft ActiveX control allows a remote attacker to execute a malicious cabinet file via an attachment and an embedded script in an HTML mail, aka the "Active Setup Control" vulnerability.
CVE-2010-1192	libESMTP, probably 1.0.4 and earlier, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
CVE-1999-1164	Microsoft Outlook client allows remote attackers to cause a denial of service by sending multiple email messages with the same X-UIDL headers, which causes Outlook to hang.
CVE-	Unspecified vulnerability in PowerPoint in Microsoft Office 2000, Office 2002, Office 2003, Office 2004 for Mac, and Office v.X for Mac

2006-3877	allows user-assisted attackers to execute arbitrary code via an unspecified "crafted file," a different vulnerability than CVE-2006-3435, CVE-2006-4694, and CVE-2006-3876.
CVE-2006-1305	Microsoft Outlook 2000, 2002, and 2003 allows user-assisted remote attackers to cause a denial of service (memory exhaustion and interrupted mail recovery) via malformed e-mail header information, possibly related to (1) long subject lines or (2) large numbers of recipients in To or CC headers.
CVE-2000-0756	Microsoft Outlook 2000 does not properly process long or malformed fields in vCard (.vcf) files, which allows attackers to cause a denial of service.
CVE-2002-1255	Microsoft Outlook 2002 allows remote attackers to cause a denial of service (repeated failure) via an email message with a certain invalid header field that is accessed using POP3, IMAP, or WebDAV, aka "E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail."
CVE-2002-0659	The ASN1 library in OpenSSL 0.9.6d and earlier, and 0.9.7-beta2 and earlier, allows remote attackers to cause a denial of service via invalid encodings.
CVE-2013-3905	Microsoft Outlook 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT does not properly expand metadata contained in S/MIME certificates, which allows remote attackers to obtain sensitive network configuration and state information via a crafted certificate in an e-mail message, aka "S/MIME AIA Vulnerability."
CVE-2007-2225	A component in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle certain HTTP headers when processing MHTML protocol URLs, which allows remote attackers to obtain sensitive information from other Internet Explorer domains, aka "URL Parsing Cross Domain Information Disclosure Vulnerability."
CVE-2004-0503	Microsoft Outlook 2003 allows remote attackers to bypass the default zone restrictions and execute script within media files via a Rich Text Format (RTF) message containing an OLE object for the Windows Media Player, which bypasses Media Player's setting to disallow scripting and may lead to unprompted installation of an executable when exploited in conjunction with predictable-file-location exposures such as CVE-2004-0502.
CVE-2010-3213	Cross-site request forgery (CSRF) vulnerability in Microsoft Outlook Web Access (owa/ev.owa) 2007 through SP2 allows remote attackers to hijack the authentication of e-mail users for requests that perform Outlook requests, as demonstrated by setting the auto-forward rule.
CVE-2008-2248	Cross-site scripting (XSS) vulnerability in Outlook Web Access (OWA) for Exchange Server 2003 SP2 allows remote attackers to inject arbitrary web script or HTML via unspecified HTML, a different vulnerability than CVE-2008-2247.
CVE-2001-0945	Buffer overflow in Outlook Express 5.0 through 5.02 for Macintosh allows remote attackers to cause a denial of service via an e-mail message that contains a long line.
CVE-2008-1448	The MHTML protocol handler in a component of Microsoft Outlook Express 5.5 SP2 and 6 through SP1, and Windows Mail, does not assign the correct Internet Explorer Security Zone to UNC share pathnames, which allows remote attackers to bypass intended access restrictions and read arbitrary files via an mhtml: URI in conjunction with a redirection, aka "URL Parsing Cross-Domain Information Disclosure Vulnerability."
CVE-2010-1194	The match_component function in smtp-tls.c in libESMTP 1.0.3.r1, and possibly other versions including 1.0.4, treats two strings as equal if one is a substring of the other, which allows remote attackers to spoof trusted certificates via a crafted subjectAltName.
CVE-1999-1016	Microsoft HTML control as used in (1) Internet Explorer 5.0, (2) FrontPage Express, (3) Outlook Express 5, and (4) Eudora, and possibly others, allows remote malicious web site or HTML emails to cause a denial of service (100% CPU consumption) via large HTML form fields such as text inputs in a table cell.
CVE-2001-0999	Outlook Express 6.00 allows remote attackers to execute arbitrary script by embedding SCRIPT tags in a message whose MIME content type is text/plain, contrary to the expected behavior that text/plain messages will not run script.
CVE-2006-0002	Unspecified vulnerability in Microsoft Outlook 2000 through 2003, Exchange 5.0 Server SP2 and 5.5 SP4, Exchange 2000 SP3, and Office allows remote attackers to execute arbitrary code via an e-mail message with a crafted Transport Neutral Encapsulation Format (TNEF) MIME attachment, related to message length validation.
CVE-2002-1090	Buffer overflow in read_smtp_response of protocol.c in libesmtp before 0.8.11 allows a remote SMTP server to (1) execute arbitrary code via a certain response or (2) cause a denial of service via long server responses.
CVE-2004-2694	Microsoft Outlook Express 6.0 allows remote attackers to bypass intended access restrictions, load content from arbitrary sources into the Outlook context, and facilitate phishing attacks via a "BASE HREF" with the target set to "_top".