



Exchange Server Bug List

Novell 顧問服務團隊-采易資訊系統(股)公司

- [VU#275193](#)04/12/2005Microsoft Exchange Server contains unchecked buffer in SMTP extended verb handling
[VU#796584](#)03/01/2001Microsoft Windows 2000 Internet Information Server (IIS) and Exchange 2000 vulnerable to DoS via malformed URL (MS01-014)
[VU#422156](#)10/15/2003Microsoft Exchange Server fails to properly handle specially crafted SMTP extended verb requests
[VU#303452](#)05/09/2006Microsoft Exchange fails to properly handle vCal and iCal properties
[VU#252146](#)01/10/2006Microsoft Outlook and Microsoft Exchange TNEF decoding buffer overflow
[VU#530660](#)11/14/2003Microsoft Exchange Server 2003 fails to assign user credentials to proper mailbox
[VU#763400](#)07/16/2001Microsoft Exchange LDAP Service is vulnerable to denial-of-service attacks
[VU#779163](#)05/29/2002Microsoft Exchange 2000 exhausts server resources while attempting to process malformed mail attributes
[VU#300373](#)06/14/2005Microsoft Outlook Web Access vulnerable to cross-site scripting
[VU#149424](#)06/06/2001Outlook Web Access (OWA) executes scripts contained in email attachment opened via Microsoft Internet Explorer (IE)
[VU#978131](#)02/07/2002Microsoft Exchange 2000 system attendant sets incorrect remote registry permissions
[VU#343145](#)05/08/2007Microsoft Exchange Server fails to properly decode MIME email messages
[VU#124113](#)05/08/2007Microsoft Exchange Outlook Web Access UTF character set label script injection vulnerability
[VU#927889](#)02/08/2005Microsoft OLE buffer overflow
[VU#948750](#)08/10/2004Microsoft Outlook Web Access contains vulnerability in HTML redirection query
[VU#886601](#)09/03/2002Internet Key Exchange (IKE) protocol discloses identity when Aggressive Mode shared secret authenticates
[VU#287771](#)08/08/2005Microsoft Outlook Web Access for Exchange Server script injection vulnerability
[VU#389665](#)08/08/2005Microsoft Exchange (IKE) implementations do not properly handle IKE response packets
[VU#552398](#)04/07/2004KAME RADIUS implementations do not properly handle IKE response packets
[VU#111947](#)09/06/2001Microsoft Exchange Outlook Web Access fails to authenticate users when searching the Global Address List
[VU#477960](#)05/12/2006WeOnlyDo! Software wodSSHServer ActiveX component fails to properly validate key exchange algorithm strings
[VU#226364](#)11/14/2005Multiple vulnerabilities in Internet Key Exchange (IKE) version 1 implementations
[VU#150236](#)04/13/2004Microsoft Windows Secure Sockets Layer (SSL) library vulnerable to DoS
[VU#874115](#)02/27/2002Microsoft Windows SMTP Service fails to properly handle responses from the NTLM authentication layer
[VU#258390](#)05/03/2005Apple Mac OS X with Bluetooth enabled may allow file exchange without prompting users
[VU#581068](#)03/17/2005NotifyLink server provides inadequate protection for cryptographic key material
[VU#520586](#)05/28/2008OpenSSL TLS handshake Denial of Service
[VU#361180](#)03/18/2005McAfee Scan Engine vulnerable to buffer overflow in LHA decoder
[VU#107280](#)02/05/2001Microsoft Windows 2000 Network Dynamic Data Exchange (DDE) executes code as Local System
[VU#873334](#)02/04/2004Check Point ISAKMP vulnerable to buffer overflow via Certificate Request
[VU#520718](#)02/09/2006BlackBerry Enterprise Server fails to properly handle Microsoft Word attachments
[VU#344900](#)04/06/2005Cisco IOS Easy VPN Server may allow unauthorized users to complete XAUTH authentication
[VU#131828](#)03/17/2005NotifyLink web client fails to adequately restrict access to administrative functions
[VU#770532](#)03/17/2005NotifyLink administrative interface displays user passwords in clear text
[VU#689326](#)01/26/2005Cisco IOS vulnerable to DoS via malformed BGP packet
[VU#349113](#)03/19/2004isakmpd fails to handle ISAKMP packets with "Payload Length" of zero
[VU#435444](#)10/15/2003Microsoft Outlook Web Access (OWA) contains cross-site scripting vulnerability in the "Compose New Message" form
[VU#432097](#)07/12/2004Novell Bordermanager VPN Service denial-of-service vulnerability
[VU#524497](#)03/19/2004isakmpd crashes when handling ISAKMP packets with malformed "Delete Payload"
[VU#223273](#)03/19/2004Integer underflow vulnerability in isakmpd "Certificate Request Payload" handling
[VU#784540](#)06/16/2004BGP implementations do not adequately handle malformed BGP OPEN and UPDATE messages
[VU#869548](#)05/19/2003Apple Mac OS X IPsec mechanism fails to handle certain incoming security policies that match by port
[VU#785945](#)03/19/2004isakmpd crashes when handling ISAKMP packets with malformed "Security Association Payload"
[VU#671028](#)05/14/2007OPeNDAP filesystem enumeration vulnerability
[VU#959203](#)12/27/2002Cisco IOS OSPF neighbor IO buffer overflow
[VU#473108](#)10/03/2003Cisco Lightweight Extensible Authentication Protocol (LEAP) uses passwords that are vulnerable to dictionary attacks
[VU#996177](#)03/19/2004Multiple memory leak vulnerabilities in isakmpd
[VU#547820](#)10/10/2003Microsoft Windows DCOM/RPC vulnerability

69個漏洞

Novell 顧問服務團隊-采易資訊系統(股)公司



Outlook Client Bug List

Novell 顧問服務團隊-采易資訊系統(股)公司

- [VU#131569](#)07/12/2001Microsoft Outlook View Control allows execution of arbitrary code and manipulation of user data
[VU#869640](#)07/13/2004Microsoft Outlook Express fails to properly validate malformed e-mail headers
[VU#305206](#)03/09/2004Microsoft Outlook fails to properly filter parameters passed via "mailto:" URL
[VU#637760](#)10/12/2004Microsoft Internet Explorer Install Engine contains a buffer overflow vulnerability
[VU#393305](#)03/11/2008Microsoft Office mailto URI remote code execution
[VU#61743601](#)09/2007Microsoft Outlook vulnerable to DoS via a malformed email message
[VU#25214601](#)10/2006Microsoft Outlook and Microsoft Exchange TNEF decoding buffer overflow
[VU#13061406](#)14/2005Microsoft Outlook Express vulnerable to remote code execution
[VU#30037306](#)14/2005Microsoft Outlook Web Access vulnerable to cross-site scripting
[VU#58029902](#)08/2005Microsoft Internet Explorer contains URL decoding cross-domain vulnerability
[VU#84377102](#)08/2005Microsoft Internet Explorer contains a DHTML method heap memory corruption vulnerability
[VU#24472912](#)03/2002Microsoft Internet Explorer does not adequately validate window ornament parameters in dialog frames
[VU#82326006](#)22/2003Microsoft Windows HTML conversion library vulnerable to buffer overflow
[VU#20726407](#)11/2004Microsoft Internet Explorer does not properly handle function redirection
[VU#25178805](#)08/2003Microsoft Internet Explorer does not safely handle multiple file download requests
[VU#87667803](#)22/2006Microsoft Internet Explorer createTextRange() vulnerability
[VU#16502201](#)13/2003Microsoft Log Sink Class ActiveX control incorrectly marked "safe for scripting"
[VU#35660012](#)15/2004Microsoft Internet Explorer DHTML Editing ActiveX control contains a cross-domain vulnerability
[VU#43544410](#)15/2003Microsoft Outlook Web Access (OWA) contains cross-site scripting vulnerability in
[VU#228302](#)11/2002Microsoft Internet Explorer allows mouse events to manipulate window
[VU#94875008](#)10/2004Microsoft Internet Explorer HTML rendering engine directive
[VU#78410211](#)25/2003Microsoft Internet Explorer query
[VU#32051606](#)25/2003Windows Media Library
[VU#84216011](#)02/2004Microsoft Internet Explorer elements
[VU#14089809](#)09/2002Microsoft Java implementation allows execution of malicious code
[VU#49070810](#)21/2001Microsoft Internet Explorer window.createPopup() method creates chromeless windows
[VU#48972102](#)26/2003Microsoft Windows Me and XP Help and Support Center does not adequately validate hcp:// URI parameters
[VU#16209710](#)22/2002Microsoft Internet Explorer does not adequately validate references to cached objects and methods
[VU#20805205](#)01/2003Microsoft Internet Explorer and Outlook Express MHTML rendering engine incorrectly executes script in Local Computer Zone
[VU#45728106](#)12/2007Microsoft Windows Win32 API fails to properly validate function parameters
[VU#71184304](#)17/2002Microsoft Internet Explorer contains cross-site scripting vulnerabilities in local HTML resources
[VU#12411305](#)08/2007Microsoft Exchange Outlook Web Access UTF character set label script injection vulnerability
[VU#61356402](#)13/2007Microsoft Internet Explorer fails to properly interpret certain responses from FTP servers
[VU#82113907](#)10/2002Network Associates PGP Outlook Plug-in contains buffer overflow in decoding mechanism
[VU#86594008](#)20/2003Microsoft Internet Explorer does not properly evaluate "application/hta" MIME type referenced by DATA attribute of OBJECT element
[VU#32641209](#)10/2003Microsoft Internet Explorer execCommand method does not properly validate URL source
[VU#65245209](#)10/2003Microsoft Internet Explorer does not adequately validate javascript: protocol URL
[VU#71387806](#)03/2004Microsoft Internet Explorer does not properly validate source of redirected frame
[VU#81320808](#)20/2003Microsoft Internet Explorer does not properly render input type tag
[VU#11194709](#)06/2001Microsoft Exchange Outlook Web Access fails to authenticate users when searching the Global Address List
[VU#93652911](#)16/2007Microsoft Jet Engine stack buffer overflow
[VU#82987605](#)09/2008Microsoft Outlook Web Access may not use the no-store HTTP directive
[VU#47690001](#)09/2007Microsoft Outlook fails to properly process a VEVENT record
[VU#27186001](#)09/2007Microsoft Outlook fails to properly parse Office Saved Searches (.oss) files
[VU#12208401](#)09/2007Microsoft Internet Explorer VML buffer overflow
[VU#77160409](#)10/2003Microsoft Internet Explorer does not properly validate URL sources
[VU#13818806](#)13/2006Microsoft Outlook Web Access for Exchange Server script injection vulnerability
[VU#14942406](#)06/2001Outlook Web Access (OWA) executes scripts contained in email attachment opened via Microsoft Internet Explorer (IE)
[VU#3562605](#)12/2000Office 2000 UA Control incorrectly marked safe for scripting

65個漏洞



Novell 顧問服務團隊-采易資訊系統(股)公司

GroupWise Server and Client Bug List

- [VU#726891](#) 08/14/2001 Novell Groupwise contains protocol implementation vulnerability allowing email to be viewed by unauthorized user
- [VU#341539](#) 10/15/2001 Novell GroupWise Server web-based front-end does not adequately validate user input thereby allowing directory traversal
- [VU#796956](#) 10/03/2006 Novell GroupWise Messenger fails to properly handle HTTP POST requests
- [VU#770532](#) 03/17/2005 NotifyLink web client fails to adequately restrict access to certain functions
- [VU#770532](#) 03/17/2005 NotifyLink web client interface displays user passwords in clear text
- [VU#795612](#) 02/26/2005 Gaim vulnerable to DoS via specially crafted HTML
- [VU#839280](#) 02/17/2005 Gaim vulnerable to malformed SNAC packet infinite processing loop
- [VU#523888](#) 02/17/2005 Gaim vulnerable to HTML processing denial of service
- [VU#520718](#) 02/09/2006 BlackBerry Enterprise Server fails to properly handle Microsoft Word attachments
- [VU#581068](#) 03/17/2005 NotifyLink server provides inadequate protection for cryptographic key material
- [VU#264097](#) 03/17/2005 NotifyLink contains multiple SQL injection vulnerabilities
- [VU#646976](#) 12/27/2005 RIM BlackBerry Enterprise Server Attachment Service does not properly handle PNG image f

2個漏洞



Novell 顧問服務團隊-采易資訊系統(股)公司