

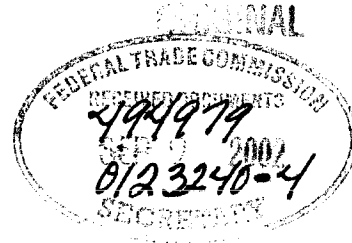
*Law Offices*  
**FOLDES & ASSOCIATES**  
PO Box 16100  
Alexandria, Virginia 22302 USA

Phone: (703) 370-0008

E-Mail: catalyst@eidmgt.com

September 6, 2002

Office of Secretary  
US Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580



**Comment: In the Matter of Microsoft Corporation – File No. 012 3240**

Honorable Commissioners:

It is respectfully submitted that Part III of the proposed Consent Order is not adequate to protect the public interest.

To assure that the public interest is adequately protected in a matter of such gravity and importance, it is essential that the monitoring entity the Commission chooses has sufficient technical domain expertise, vendor/industry independence and is sufficiently funded -- as to warrant confidence that Microsoft's online identity management, user privacy and personal information security efforts can be adequately monitored.

No such party is specified in the Proposed Agreement and Order. *Nor is there provision for – or assurance of – sufficient funding in the Proposed Order for the designated monitoring entity to properly and effectively carry out its duties.*

The Commission has at least one such highly qualified, non-profit, vendor and industry independent party available to perform such a critical monitoring role.

According to materials on its website ( enclosed pages ) Mitretek Systems has served, and currently serves, a wide array of public service clients providing Information Security and Internet Security services to the Department of Defense, and other critical national infrastructure safety tasked agencies of the US Government. See enclosed qualifications of Mitretek Systems ([www.mitretek.org](http://www.mitretek.org)) printed from its website.

Note, the undersigned has no prior or present affiliation with Mitretek Systems.

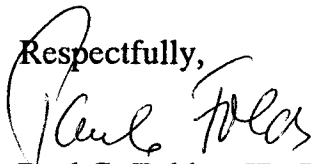
**Federal Trade Commission**  
**Comment: Microsoft, File No. 012 3240**  
**September 6, 2002**  
**Page 2**

The complexity of Internet identity management and security issues requires that a technically competent and adequately funded party be used to monitor the proposed Order for its 20-year term. The Proposed Agreement and Order does not provide such assurance currently.

**Given Microsoft's extensive history \*/ of important software security lapses, several of which have been labeled 'critical' by Microsoft itself, absent such technically qualified, vendor/industry independent and adequately funded monitoring of Microsoft, the public interest will not be adequately served. \*/ See enclosed 10 pages of security bulletins printed from Microsoft's website today -- including several critical security issues identified just in the last 60 days !**

The Commission is urged to modify its Proposed Agreement and Order to specify monitoring by a technically capable, vendor/industry independent party such as Mitretek, or similarly qualified organization -- that is sufficiently funded by Microsoft during the term of the Order so that it can perform its task adequately.

Respectfully,



Paul G. Foldes JD, BE (Elec. Eng.)  
Former FTC Bureau of Consumer Protection Attorney

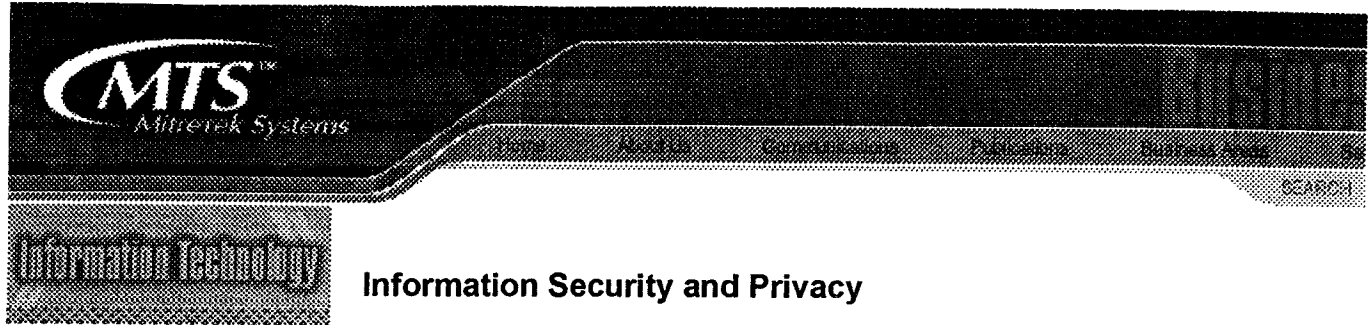
*Enclosures*

- 1) Web pages relating Mitretek's expertise regarding critical Internet infrastructure and user security, and educational services for network operators and end users
- 2) Copies of web pages from Microsoft's current web site relating to 'Security Bulletins'
- 3) Internet News, August 13, 2002 reporting on Microsoft Internet Explorer security flaw endangering consumers who bank online or shop at e-commerce web sites

*Delivery*

US Mail, First Class, Certified, Receipt: 7000 0600 0027 5734 7776

Via Fax / to assure timely receipt, given recent publicly reported delays in surface mail deliveries to government agencies in downtown Washington



- Criminal Justice**
- Environment & Energy**
- Healthcare**
- Homeland Security & Counterterrorism**
- Information Technology**
  - Engineering Management
  - Information Security and Privacy
  - Acquisition Support & Economic Analysis
  - e-Government
  - Knowledge Management
  - Systems Engineering
  - Biometric Identification
- Oceans, Atmosphere and Space**
- Telecommunications**
- Toxicology and Risk Assessment**
- Transportation**

## Information Security and Privacy

- [National Security](#)
- [Network Security Engineering](#)
- [Risk Management](#)
- [Security Assessment](#)
- [Security Awareness](#)
- [Security Policy Analysis](#)
- [Internet Security](#)

### National Security ✓

Mitretek has been evaluating operating systems and computing system components for conformance with Orange Book Security Criteria for many years. Our independence and objectivity create confidence for vendors and system integrators that our evaluations are free of bias and ulterior motivation. As the evaluation community moves to adopt the international Common Criteria, we are helping to ensure processes maintain the high standards of the old. We assist the DOD in implementing the Common Criteria supporting methodologies by training evaluators, certifying evaluation laboratories, serving on Working Group and Technical Review Boards, writing and evaluating Common Criteria Security Protection Profiles—all to assure the technical correctness of evaluations and the consistent application of standards. Mitretek personnel have conducted Orange Book evaluations that range from Micro to the C2 security level to Wang XTS-300 at B3. Mitretek supports the InfoSec Research Council Science and Technology Study Groups. Mitretek personnel have played significant roles in the Commission on Critical Infrastructure Protection (PCCIP) development and follow-on activities. Our experience has broad applicability in government and commercial applications, from the least critical.

(See [Homeland Security for more information](#))

### Network Security Engineering

Mitretek's network security engineering experience can help you realize the potential of Internet business by avoiding the pitfalls—protecting your business and keeping your customers' confidence. Internet business opportunities often carry a significant potential for adding new security vulnerabilities, in the form of unauthorized release of privileged information, modification of data, identity masquerading, in the form of computer viruses or other hostile code, and system downtime. Our network security experience can help your Internet business or government application online with a minimum risk of security problems.

### Risk Management

Mitretek's extensive risk management experience can be applied to identify and reduce risk in the implementation or enhancement of new systems. System designers without computer security expertise create systems and with the increasing use of networking, very few systems can survive insecurity. Yet this is nearly every government modernization project, even those based on the use of commercial components.

### Security Assessment ✓

A Mitretek security assessment is a two-step process: a threat analysis followed by a vulnerability analysis. The threat analysis identifies the assets that require protection and the vulnerability analysis uncovers computer and network weaknesses that need to be strengthened. The threat analysis requires infrastructure and determining the threats to which it is vulnerable. The emphasis is on correlating threats to specific environments so that the best use is made of information security resources. The vulnerability analysis identifies security-related weaknesses in the system. Using both manual methods and automated tools, the team looks for vulnerabilities that are exploitable. If desired, this analysis can be supplemented by penetration of the system.

### Security Awareness ✓

Mitretek's technical staff can create custom security courses, ranging from one day to many system administrators, security managers and anyone who wants to understand computer security and the security characteristics of a particular system. Awareness of security issues by those who implement, operate, and use computing systems is critical to overall security. These classes cover other security activities and can be tailored to the needs of a wide range of application domains (e.g., finance, defense, public service, intelligence).

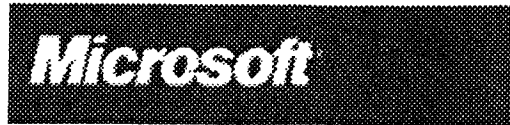
### Security Policy Analysis

Mitretek develops security policies for a broad range of systems, including those in healthcare, public service, government, and defense. We also evaluate existing policies for continued applicability in a constantly changing security environment. Policies reflect both domain-specific security concerns and general security issues of preserving information integrity, safeguarding against improper information disclosure, ensuring the availability of information. Policies identify and categorize the types of data involved, the individuals who are permitted to access information and what access restrictions should be placed on remote access, how the system is protected from malicious use, and proper user authentication procedures. Physical security is often included, as well.

### Internet Security ✓

Mitretek's knowledge of Internet protocols, technologies, and attacks allows us to help our customers understand the issues behind the jargon and the marketing hype, and to anticipate and mitigate security vulnerabilities in applications they deploy. Our vendor-independent perspective and broad technical knowledge allow us to solve tough security problems and do it objectively and provide unbiased advice. Our experience in securing our own Internet connected infrastructure can be applied to our customers' systems.

Send mail to [bernard.parker@mitretek.org](mailto:bernard.parker@mitretek.org) with questions or comments.  
Copyright © 1996-2002 Mitretek Systems  
Last modified: 07/18/2002



Security & Privacy Home | Site Map | Security Worldwide

Search

Advanced Search

Security & Privacy Home
IT Professionals (TechNet)
Developers (MSDN)
Home Users
Businesses
Services
Communities
Partners

### Free Support

Call  
**1-800-PCSAFETY**  
for free virus-related support  
(U.S. and Canada only)

Please call your local Microsoft subsidiary.  
Find your subsidiary

## Security & Privacy



### Important Announcements

- ▶ [Information about reported Web security vulnerability in Microsoft® Internet Explorer Secure Sockets Layer \(SSL\) implementation](#)
- ▶ [Q&A: Microsoft seeks industrywide collaboration for "Palladium" initiative](#)



#### for IT professionals

Get tools, checklists, best practices, planning, and training to help you do your job and manage your networks securely.

- [Microsoft patterns and practices provide detailed technical guidance](#)
- [Wireless and mobile security: Technical resources for IT professionals](#)
- [More security resources for IT professionals on Microsoft TechNet...](#)



#### for developers

Keep your skills sharp for creating secure software. Microsoft offers core documentation, code samples, technical articles, and other resources for software designers, coders, and testers.

- [Defend your code with the top 10 security tips every developer must know](#)
- [Code Secure: "Cross-Site Scripting Explained" by Michael Howard, author of Writing Secure Code](#)
- [More security resources for developers on MSDN@...](#)



#### for home users

Keep up-to-date on protecting the privacy of your personal information and safeguarding your desktop computer, laptop, mobile devices, or small network.

- [Follow 7 steps to personal computing security](#)
- [Get the most from Microsoft Windows® Update](#)
- [More on security and privacy for home users...](#)



#### for businesses

How well your company safeguards information can be a competitive asset or a liability. Stay current on strategies and opportunities for keeping your organization secure.

- [Understand Microsoft's security and Trustworthy Computing Initiatives](#)
- [Upgrade your security: Tips for small businesses](#)
- [More security resources for businesses...](#)



### security bulletins

**September 4, 2002** ✓

[MS02-050 Certificate Validation Flaw Could Enable Identity Spoofing \(Q328145\)](#)

- \* For Windows 98, 98 Second Edition; Windows Me; Windows NT 4.0; Windows NT 4.0, Terminal Server Edition; Windows 2000; Windows XP; Office for Mac; Internet Explorer for Mac; Outlook Express for Mac

[MS02-049 Flaw Could Enable Web Page to Launch Visual FoxPro Without Warning \(Q326568\)](#)

- \* For Visual FoxPro 6.0

[Search for Bulletins and Patches](#)

[Report a Security Vulnerability](#)

### virus alerts

**July 31, 2002**

[w32.Chir.B@mm virus](#)

- \* Affects Outlook, Outlook Express, and Web-based e-mail programs

**July 15, 2002**

[W32.Frethem viruses](#)

- \* Affects Outlook, Outlook Express, and Web-based e-mail programs

**April 17, 2002**

[Klez.H and variants](#)

- \* Affects Outlook, Outlook Express, and Web-based e-mail programs

[More Virus Alerts...](#)

[Virus Protection Strategies for IT Professionals](#)

TechNet Home > Security

## HotFix & Security Bulletin Service

Register To Automatically Receive Security Bulletins.

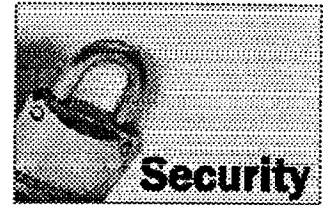
### Search by Product and Service Pack

Select the Product and Service Pack you are running to view the security bulletins that are available for your system. (More information on how to use this feature is available in the [Search Tool FAQ](#)).

Product:

Service Pack:

OR



#### Security Administration

- [Best Practices](#)
- [Database](#)
- [Internet/Intranet](#)
- [Messaging and Collaboration](#)
- [Network](#)

### Search by Knowledge Base Article

Enter a Knowledge Base article number to view any security bulletins associated with it.

Knowledge base article number (e.g. Q123456):

#### Hot Fix Central

- [HotFix & Bulletin Search](#)
- [E-Mail Notification](#)
- [Service Packs](#)

### September 2002

[MS02-050 : Certificate Validation Flaw Could Enable Identity Spoofing \(Q328145\)](#) ✓

[MS02-049 : Flaw Could Enable Web Page to Launch Visual FoxPro 6.0 Application Without Warning \(Q326568\)](#)

### August 2002

[MS02-048 : Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates \(Q323172\)](#) ✓

[MS02-047 : Cumulative Patch for Internet Explorer \(Q323759\)](#)

[MS02-046 : Buffer Overrun in TSAC ActiveX Control Could Allow Code Execution \(Q327521\)](#)

[MS02-045 : Unchecked Buffer in Network Share Provider can lead to Denial of Service \(Q326830\)](#) ✓

[MS02-044 : Unsafe Functions in Office Web Components \(Q328130\)](#)

[MS02-043 : Cumulative Patch for SQL Server \(Q316333\)](#)

[MS02-042 : Flaw in Network Connection Manager Could Enable Privilege Elevation \(Q326886\)](#)

[MS02-041 : Unchecked Buffer in Content Management Server Could Enable Server Compromise \(Q326075\)](#) ✓

#### Security Resources

- [Developers](#)
- [Newsgroups](#)
- [Anti-Virus](#)
- [Books](#)
- [Case Studies](#)
- [Columns](#)
- [Government Issues](#)
- [Microsoft Policies](#)
- [Partners](#)
- [Products and Technologies](#)
- [Tools and Checklists](#)
- [Training](#)
- [Web Sites](#)
- [Contact Microsoft Security](#)

### July 2002

[MS02-040 : Unchecked Buffer in MDAC Function Could Enable SQL Server Compromise \(Q326573\)](#)

[MS02-039 : Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution \(Q323875\)](#)

[MS02-038 : Unchecked Buffer in SQL Server 2000 Utilities Could Allow Code Execution \(Q316333\)](#)

[MS02-037 : Server Response To SMTP Client EHLO Command Results In Buffer Overrun \(Q326322\)](#)

[MS02-036 : Authentication Flaw in Microsoft Metadirectory Services Could Allow Privilege Elevation \(Q317138\)](#)

[MS02-035 : SQL Server Installation Process May Leave Passwords on System \(Q263968\)](#)

[MS02-034 : Cumulative Patch for SQL Server \(Q316333\)](#)

### June 2002

[MS02-033 : Unchecked Buffer in Profile Service Could Allow Code Execution in Commerce Server \(Q322273\)](#)

[MS02-032 : Cumulative Patch for Windows Media Player \(Q320920\)](#)

[MS02-031 : Cumulative Patches for Excel and Word for Windows \(Q324458\)](#)

[MS02-030 : Unchecked Buffer in SQLXML Could Lead to Code Execution \(Q321911\)](#)

[MS02-029 : Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution \(Q318138\)](#)

[MS02-028 : Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise \(Q321599\)](#)

[MS02-027 : Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice \(Q323889\)](#)

[MS02-026 : Unchecked Buffer in ASP.NET Worker Process \(Q322289\)](#)

## **May 2002**

---

[MS02-025 : Malformed Mail Attribute Can Cause Exchange 2000 to Exhaust CPU Resources \(Q320436\)](#)

[MS02-024 : Authentication Flaw in Windows Debugger Can Lead to Elevated Privileges \(Q320206\)](#)

[MS02-023 : 15 May 2002 Cumulative Patch for Internet Explorer \(Q321232\)](#)

[MS02-022 : Unchecked Buffer in MSN Chat Control Can Lead to Code Execution \(Q321661\)](#)

## **April 2002**

---

[MS02-021 : E-mail Editor Flaw Could Lead to Script Execution on Reply or Forward \(Q321804\)](#)

[MS02-020 : SQL Extended Procedure Functions Contain Unchecked Buffers \(Q319507\)](#)

[MS02-019 : Unchecked Buffer in Internet Explorer and Office for Mac Can Cause Code to Execute \(Q321309\)](#)

[MS02-018 : Cumulative Patch for Internet Information Service \(Q319733\)](#)

[MS02-017 : Unchecked Buffer in the Multiple UNC Provider Could Enable Code Execution \(Q311967\)](#)

[MS02-016 : Opening Group Policy Files for Exclusive Read Blocks Policy Application \(Q318593\)](#)

## **March 2002**

---

[MS02-015 : 28 March 2002 Cumulative Patch for Internet Explorer](#)

[MS02-014 : Unchecked Buffer in Windows Shell Could Lead to Code Execution](#)

[MS02-013 : 04 March 2002 Cumulative VM Update](#)

## **February 2002**

---

[MS02-012 : Malformed Data Transfer Request Can Cause Windows SMTP Service to Fail](#)

[MS02-011 : Authentication Flaw Could Allow Unauthorized Users To Authenticate To SMTP Service](#)

[MS02-010 : Unchecked Buffer in ISAPI Filter Could Allow Commerce Server Compromise](#)

[MS02-009 : Incorrect VBScript Handling in IE Can Allow Web Pages to Read Local Files](#)

[MS02-008 : XMLHTTP Control Can Allow Access to Local Files](#)

[MS02-007 : SQL Server Remote Data Source Function Contain Unchecked Buffers](#)

[MS02-006 : Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run](#)

[MS02-005 : 11 February 2002 Cumulative Patch for Internet Explorer](#)

[MS02-004 : Unchecked Buffer in Telnet Server Could Lead to Arbitrary Code Execution](#)

[MS02-003 : Exchange 2000 System Attendant Incorrectly Sets Remote Registry Permissions](#)

[MS02-002 : Malformed Network Request Can Cause Office v. X for Mac to Fail](#)

## **January 2002**

---

[MS02-001 : Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data](#)

## **December 2001**

---

MS01-060 : SQL Server Text Formatting Functions Contain Unchecked Buffers

MS01-059 : Unchecked Buffer in Universal Plug and Play Can Lead to System Compromise

MS01-058 : 13 December 2001 Cumulative Patch for IE

MS01-057 : Specially Formed Script in HTML Mail Can Execute in Exchange 5.5 OWA

### **November 2001**

---

MS01-056 : Windows Media Player .ASF Processor Contains Unchecked Buffer

MS01-055 : 13 November 2001 Cumulative Patch for IE

MS01-054 : Invalid Universal Plug and Play Request Can Disrupt System Operation

### **October 2001**

---

MS01-053 : Downloaded Applications Can Execute on Mac IE 5.1 for OS X

MS01-052 : Invalid RDP Data Can Cause Terminal Service Failure

MS01-051 : Malformed Dotless IP Address Can Cause Web Page to be Handled in Intranet Zone

MS01-050 : Malformed Excel or PowerPoint Document Can Bypass Macro Security

### **September 2001**

---

MS01-049 : Deeply-nested OWA Request Can Consume Server CPU Availability

MS01-048 : Malformed Request to RPC Endpoint Mapper Can Cause RPC Service to Fail

MS01-047 : OWA Function Allows Unauthenticated User to Enumerate Global Address List

### **August 2001**

---

MS01-046 : Access Violation in Windows 2000 IRDA Driver Can Cause System to Restart

MS01-045 : ISA Server H.323 Gatekeeper Service Contains Memory Leak

MS01-044 : 15 August 2001 Cumulative Patch for IIS

MS01-043 : NNTP Service in Windows NT 4.0 and Windows 2000 Contains Memory Leak

### **July 2001**

---

MS01-042 : Windows Media Player .NSC Processor Contains Unchecked Buffer

MS01-041 : Malformed RPC Request Can Cause Service Failure

MS01-040 : Invalid RDP Data Can Cause Memory Leak in Terminal Services

MS01-039 : Services for Unix 2.0 Telnet and NFS Services Contain Memory Leaks

MS01-038 : Outlook View Control Exposes Unsafe Functionality

MS01-037 : Authentication Error in SMTP Service Could Allow Mail Relaying

### **June 2001**

---

MS01-036 : Function Exposed via LDAP over SSL Could Enable Passwords to be Changed

MS01-035 : FrontPage Server Extension Sub-Component Contains Unchecked Buffer

MS01-034 : Malformed Word Document Could Enable Macro to Run Automatically

MS01-033 : Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise

MS01-032 : SQL Query Method Enables Cached Administrator Connection to be Reused

MS01-031 : Predictable Named Pipes Could Enable Privilege Elevation via Telnet

MS01-030 : Incorrect Attachment Handling in Exchange OWA Can Execute Script

### **May 2001**



---

MS01-029 : Windows Media Player .ASX Processor Contains Unchecked Buffer

MS01-028 : RTF Document Linked to Template Can Run Macros Without Warning

MS01-027 : Flaws In Web Server Certificate Validation Could Enable Spoofing

MS01-026 : 14 May 2001 Cumulative Patch for IIS

MS01-025 : Index Server Search Function Contains Unchecked Buffer

MS01-024 : Malformed Request to Domain Controller Can Cause Memory Exhaustion

MS01-023 : Unchecked Buffer in ISAPI Extension Could Enable Compromise of IIS 5.0 Server

### **April 2001**

---

MS01-022 : WebDAV Service Provider Can Allow Scripts to Levy Requests as User

MS01-021 : Web Request Can Cause Access Violation in ISA Server Web Proxy Service

### **March 2001**

---

MS01-020 : Incorrect MIME Header Can Cause IE to Execute E-mail Attachment

MS01-019 : Passwords for Compressed Folders are Recoverable

MS01-018 : Visual Studio VB-TSQL Object Contains Unchecked Buffer

MS01-017 : Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard ✓

MS01-016 : Malformed WebDAV Request Can Cause IIS to Exhaust CPU Resources

MS01-015 : IE Can Divulge Location of Cached Content

MS01-014 : Malformed URL Can Cause Service Failure in IIS 5.0 and Exchange 2000

### **February 2001**

---

MS01-013 : Windows 2000 Event Viewer Contains Unchecked Buffer

MS01-012 : Outlook - Outlook Express VCard Handler Contains Unchecked Buffer

MS01-011 : Malformed Request to Domain Controller Can Cause CPU Exhaustion

MS01-010 : Windows Media Player Skins Files Can Enable Java Code to Execute

MS01-009 : Malformed PPTP Packet Stream Can Cause Kernel Exhaustion

MS01-008 : Malformed NTLMSSP Request Can Enable Code to Run with System Privileges

MS01-007 : Network DDE Agent Requests Can Enable Code to Run in System Context

### **January 2001**

---

MS01-006 : Invalid RDP Data Can Cause Terminal Server Failure

MS01-005 : Packaging Anomaly Could Cause Hotfixes to be Removed

MS01-004 : Malformed .HTR Request Allows Reading of File Fragments

MS01-003 : Weak Permissions on Winsock Mutex Can Allow Service Failure

MS01-002 : PowerPoint 2000 File Parser Contains Unchecked Buffer

MS01-001 : Web Client Will Perform NTLM Authentication Regardless of Security Settings

### **December 2000**

---

MS00-100 : Malformed Web Form Submission Vulnerability

MS00-099 : Directory Service Restore Mode Password Vulnerability

MS00-098 : Indexing Service File Enumeration Vulnerability

MS00-097 : Severed Windows Media Server Connection Vulnerability

[MS00-096 : SNMP Parameters Vulnerability](#)

[MS00-095 : Registry Permissions Vulnerability](#)

[MS00-094 : Phone Book Service Buffer Overflow Vulnerability](#)

[MS00-093 : Browser Print Template and File Upload via Form Vulnerabilities](#)

[MS00-092 : Extended Stored Procedure Parameter Parsing Vulnerability](#)

### **November 2000**

---

[MS00-091 : Incomplete TCP/IP Packet Vulnerability](#)

[MS00-090 : .ASX Buffer Overrun and .WMS Script Execution Vulnerabilities](#)

[MS00-089 : Domain Account Lockout Vulnerability](#)

[MS00-088 : Exchange User Account Vulnerability](#)

[MS00-087 : Terminal Server Login Buffer Overflow Vulnerability](#)

[MS00-086 : Web Server File Request Parsing Vulnerability](#)

[MS00-085 : ActiveX Parameter Validation Vulnerability](#)

[MS00-084 : Indexing Services Cross Site Scripting Vulnerability](#)

[MS00-083 : Netmon Protocol Parsing Vulnerability](#)

### **October 2000**

---

[MS00-082 : Malformed MIME Header Vulnerability](#)

[MS00-081 : New Variant of VM File Reading Vulnerability](#)

[MS00-080 : Session ID Cookie Marking Vulnerability](#)

[MS00-079 : HyperTerminal Buffer Overflow Vulnerability](#)

[MS00-078 : Web Server Folder Traversal Vulnerability](#)

[MS00-077 : NetMeeting Desktop Sharing Vulnerability](#)

[MS00-076 : Cached Web Credentials Vulnerability](#)

[MS00-075 : Microsoft VM ActiveX Component Vulnerability](#)

[MS00-074 : WebTV for Windows Denial of Service Vulnerability](#)

[MS00-073 : Malformed IPX NMPI Packet Vulnerability](#)

[MS00-072 : Share Level Password Vulnerability](#)

[MS00-071 : Word Mail Merge Vulnerability](#)

[MS00-070 : Multiple LPC and LPC Ports Vulnerabilities](#)

### **September 2000**

---

[MS00-069 : Simplified Chinese IME State Recognition Vulnerability](#)

[MS00-068 : OCX Attachment Vulnerability](#)

[MS00-067 : Windows 2000 Telnet Client NTLM Authentication Vulnerability](#)

[MS00-066 : Malformed RPC Packet Vulnerability](#)

[MS00-065 : Still Image Service Privilege Escalation Vulnerability](#)

[MS00-064 : Unicast Service Race Condition Vulnerability](#)

[MS00-063 : Invalid URL Vulnerability](#)

### **August 2000**

---

[MS00-062 : Local Security Policy Corruption Vulnerability](#)

[MS00-061 : Money Password Vulnerability](#)

[MS00-060 : IIS Cross-Site Scripting Vulnerabilities](#)

[MS00-059 : Java VM Applet Vulnerability](#)

[MS00-058 : Specialized Header Vulnerability](#)

[MS00-057 : File Permission Canoncalization Vulnerability](#)

[MS00-056 : Microsoft Office HTML Object Tag Vulnerability](#)

[MS00-055 : Scriptlet Rendering Vulnerability](#)

[MS00-054 : Malformed IPX Ping Packet Vulnerability](#)

[MS00-053 : Service Control Manager Named Pipe Impersonation Vulnerability](#)

### **July 2000**

---

[MS00-052 : Relative Shell Path Vulnerability](#)

[MS00-047 : NetBIOS Name Server Protocol Spoofing Vulnerability](#)

[MS00-051 : Excel REGISTER.ID Function Vulnerability](#)

[MS00-050 : Telnet Server Flooding Vulnerability](#)

[MS00-046 : Cache Bypass Vulnerability](#)

[MS00-045 : Persistent Mail-Browser Link Vulnerability](#)

[MS00-043 : Malformed E-mail Header Vulnerability](#)

[MS00-044 : Absent Directory Browser Argument Vulnerability](#)

[MS00-049 : Office HTML Script and IE Script Vulnerabilities](#)

[MS00-048 : Stored Procedure Permissions Vulnerability](#)

### **June 2000**

---

[MS00-042 : Active Setup Download Vulnerability](#)

[MS00-020 : Desktop Separation Vulnerability](#)

[MS00-041 : DTS Password Vulnerability](#)

[MS00-040 : Remote Registry Access Authentication Vulnerability](#)

[MS00-039 : SSL Certificate Validation Vulnerabilities](#)

[MS00-037 : HTML Help File Code Execution Vulnerability](#)

[MS00-032 : Protected Store Key Length Vulnerability](#)

### **May 2000**

---

[MS00-038 : Malformed Windows Media Encoder Request Vulnerability](#)

[MS00-035 : SQL Server 7.0 Service Pack Password Vulnerability](#)

[MS00-036 : ResetBrowser Frame and Host Announcement Frame Vulnerabilities](#)

[MS00-029 : IP Fragment Reassembly Vulnerability](#)

[MS00-033 : Frame Domain Verification and Unauthorized Cookie Access and Malformed Component Attribute Vulnerabilities](#)

[MS00-034 : Office 2000 UA Control Vulnerability](#)

[MS00-030 : Malformed Extension Data In URL Vulnerability](#)

[MS00-031 : Undelimited .HTR Request and File Fragment Reading via .HTR Vulnerabilities](#)

### **April 2000**

---

MS00-028 : Server-Side Image Map Components Vulnerability

MS00-027 : Malformed Environment Variable Vulnerability

MS00-026 : Mixed Object Access Vulnerability

MS00-025 : Link View Server-Side Component Vulnerability

MS00-024 : OffloadModExpo Registry Permissions Vulnerability

MS00-023 : Myriad Escaped Characters Vulnerability

MS00-022 : XLM Text Macro Vulnerability

### **March 2000**

---

MS00-021 : Malformed TCP/IP Print Request Vulnerability

MS00-019 : Virtualized UNC Share Vulnerability

MS00-018 : Chunked Encoding Post Vulnerability

MS00-016 : Malformed Media License Request Vulnerability

MS00-017 : DOS Device In Path Name Vulnerability

MS00-008 : Registry Permissions Vulnerability

MS00-014 : SQL Query Abuse Vulnerability

MS00-015 : Clip Art Buffer Overrun Vulnerability

### **February 2000**

---

MS00-013 : Misordered Windows Media Services Handshake Vulnerability

MS00-012 : Remote Agent Permissions Vulnerability

MS00-011 : VM File Reading Vulnerability

MS00-010 : Site Wizard Input Validation Vulnerability

MS00-009 : Image Source Redirect Vulnerability

MS00-007 : Recycle Bin Creation Vulnerability

### **January 2000**

---

MS00-006 : Malformed Hit-Highlighting Argument Vulnerability

MS00-004 : RDISK Registry Enumeration File Vulnerability

MS00-002 : Malformed Conversion Data Vulnerability

MS00-005 : Malformed RTF Control Word Vulnerability

MS00-003 : Spoofed LPC Port Request Vulnerability

MS00-001 : Malformed IMAP Request Vulnerability

### **December 1999**

---

MS99-060 : HTML Mail Attachment Vulnerability

MS99-061 : Escape Character Parsing Vulnerability

MS99-058 : Virtual Directory Naming Vulnerability

MS99-059 : Malformed TDS Packet Header Vulnerability

MS99-057 : Malformed Security Identifier Request Vulnerability

MS99-056 : Syskey Keystream Reuse Vulnerability

MS99-055 : Malformed Resource Enumeration Argument Vulnerability

MS99-050 : Server-side Page Reference Redirect Vulnerability

MS99-053 : Windows Multithreaded SSL ISAPI Filter Vulnerability

MS99-054 : WPAD Spoofing Vulnerability

**November 1999**

---

MS99-052 : Legacy Credential Caching Vulnerability

MS99-051 : IE Task Scheduler Vulnerability

MS99-049 : File Access URL Vulnerability

MS99-048 : Active Setup Control Vulnerability

MS99-047 : Malformed Spooler Request Vulnerability

**October 1999**

---

MS99-046 : Improve TCP Initial Sequence Number Randomness

MS99-045 : Virtual Machine Verifier Vulnerability

MS99-044 : Excel SYLK Vulnerability

MS99-043 : Javascript Redirect Vulnerability

MS99-042 : IFRAME ExecCommand Vulnerability

**September 1999**

---

MS99-041 : RASMAN Security Descriptor Vulnerability

MS99-040 : Download Behavior Vulnerability

MS99-039 : Domain Resolution and FTP Download Vulnerabilities

MS99-038 : Spoofed Route Pointer Vulnerability

MS99-037 : ImportExportFavorites Vulnerability

MS99-036 : Windows NT 4.0 Does Not Delete Unattended Installation File

MS99-035 : Set Cookie Header Caching Vulnerability

MS99-033 : Malformed Telnet Argument Vulnerability

MS99-034 : Fragmented IGMP Packet Vulnerability

**August 1999**

---

MS99-032 : scriptlet.typeLib/Eyedog Vulnerability

MS99-031 : Virtual Machine Sandbox Vulnerability

MS99-030 : Office ODBC Vulnerabilities

MS99-029 : Malformed HTTP Request Header Vulnerability

MS99-028 : Terminal Server Connection Request Flooding Vulnerability

MS99-027 : Encapsulated SMTP Address Vulnerability

**July 1999**

---

MS99-026 : Malformed Dialer Entry Vulnerability

MS99-025 : Unauthorized Access to IIS Servers through ODBC Data Access with RDS

MS99-024 : Unprotected IOCTLs Vulnerability

**June 1999**

---

MS99-023 : Malformed Image Header Vulnerability

MS99-022 : Double Byte Code Page Vulnerability

MS99-021 : CSRSS Worker Thread Exhaustion Vulnerability

MS99-020 : Malformed LSA Request Vulnerability

MS99-019 : Malformed HTR Request Vulnerability

**May 1999**

.....  
MS99-018 : Malformed Favorites Icon Vulnerability

MS99-017 : RAS and RRAS Password Vulnerability

MS99-016 : Malformed Phonebook Entry Vulnerability

MS99-015 : Malformed Help File Vulnerability

MS99-014 : Excel 97 Virus Warning Vulnerabilities

MS99-013 : File Viewers Vulnerability

**April 1999**

.....  
MS99-012 : MSHTML Update Available for Internet Explorer

MS99-011 : DHTML Edit Vulnerability

**March 1999**

.....  
MS99-010 : File Access Vulnerability In Personal Web Server

MS99-009 : Malformed Bind Request Vulnerability

MS99-008 : Windows NT Screen Saver Vulnerability

**February 1999**

.....  
MS99-007 : Taskpads Scripting Vulnerability

MS99-006 : Windows NT Known DLLs List Vulnerability

MS99-005 : BackOffice Server 4.0 Does Not Delete Installation Setup File

MS99-004 : Authentication Processing Error in Windows NT 4.0 Service Pack 4

MS99-003 : IIS Malformed FTP List Request Vulnerability

**January 1999**

.....  
MS99-002 : Word 97 Template Vulnerability

MS99-001 : Exposure in Forms 2.0 TextBox Control that allows data to be read from user's Clipboard

**December 1998**

.....  
MS98-020 : Frame Spoof Vulnerability

MS98-019 : IIS GET Vulnerability

MS98-018 : Excel CALL Vulnerability

**November 1998**

.....  
MS98-017 : Named Pipes Over RPC Vulnerability

**October 1998**

.....  
MS98-016 : Dotless IP Address Issue in Microsoft Internet Explorer 4

MS98-015 : Untrusted Scripted Paste Issue in Microsoft Internet Explorer 4.01

**September 1998**

[MS98-014 : RPC Spoofing Denial of Service on Windows NT](#)

[MS98-013 : Internet Explorer Cross Frame Navigate Vulnerability](#)

**August 1998**

---

[MS98-012 : Updates available for Security Vulnerabilities In Microsoft PPTP](#)

[MS98-011 : Window.External JScript Vulnerability In Microsoft Internet Explorer 4.0](#)

[MS98-010 : Information on the Back Orifice Program](#)

**July 1998**

---

[MS98-009 : Windows NT Privilege Elevation Attack](#)

[MS98-008 : Long file name Security Issue affecting Microsoft Outlook 98 and Microsoft Outlook Express 4.x](#)

[MS98-007 : Potential SMTP and NNTP Denial-of-Service Vulnerabilities](#)

[MS98-006 : Potential Denial-of-Service in IIS FTP Server due to Passive Connections](#)

[MS98-005 : Unwanted Data Issue with Office 98 for the Macintosh](#)

[MS98-004 : Unauthorized ODBC Data Access with RDS and IIS](#)

[MS98-003 : File Access Issue with Windows NT Internet Information Server](#)

**June 1998**

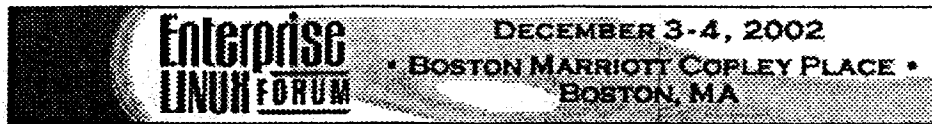
---

[MS98-002 : Error Message Vulnerability Against Secured Internet Servers](#)

[MS98-001 : Disabling Creation of Local Groups on a Domain by Non-Administrative Users](#)

[Contact Us](#) | [E-mail this Page](#) | [TechNet Newsletter](#)

© 2002 Microsoft Corporation. All rights reserved. [Terms of Use](#) [Privacy Statement](#) [Accessibility](#)



[www.internetnews.com/ec-news/article.php/1445531](http://www.internetnews.com/ec-news/article.php/1445531)

[Back to Article](#)

Latest IE Flaw an E-Commerce Threat?  
August 13, 2002

Yet another bug has been found in Microsoft's Internet Explorer browser, this one said to potentially allow the theft of data from consumers who are banking online or shopping at e-commerce Web sites.

Microsoft ([Quote](#), [Company Info](#)) is investigating, but has yet to make a formal statement or issue a fix. One security expert was quoted as saying that "the cryptographic protections of SSL don't work if you're a Microsoft IE user."

The loophole could allow hackers to trick computer users into thinking they are shopping at legitimate Web sites, exposing their credit card numbers and other personal information.

The flaw was discovered by Mike Benham, a San Francisco programmer who posted a note to the Bugtraq mailing list on the [SecurityFocus](#) Internet site, outlining what he called the possibility of an undetected "man in the middle" attack.

Some security experts said it was a serious concern; others were quoted as saying that the complexity and knowledge required to exploit the vulnerability makes the probability of widespread attacks unlikely.

Benham said in his warning that Internet Explorer versions 5.0, 5.5 and 6.0 have loopholes in handling digital certificates, such as those from VeriSign ([Quote](#), [Company Info](#)), which verify Web sites as being legitimate and also include unique code for encrypting information.

Essentially, any Web site operator with a valid certificate could pretend to be any other Web site operator, Benham said.

"I would consider this to be incredibly severe," Benham said in his posting. "Any of the standard connection hijacking techniques can be combined with this vulnerability to produce a successful man in the middle attack." Netscape has no such loophole, he said.

Microsoft reportedly is still investigating and is unsure even whether to call it a vulnerability, Scott Culp, manager of Microsoft's Security Response Center, was quoted as saying. However, Microsoft and VeriSign were said to be working together on the matter and a VeriSign spokesman said that no real cases have been reported in which someone

An advertisement for Sun Microsystems. At the top, it says "Starting at \$2,795, there's no excuse for deploying Windows at the edge of the network." Below this text is a photograph of a Sun server rack. At the bottom left of the ad is a dark button with the text "Find out more &gt;&gt;". At the bottom right is the Sun Microsystems logo, which consists of a stylized sun icon and the word "Sun" in a script font above "microsystems" in a smaller sans-serif font.



and a VeriSign spokesman said that no real cases have been reported in which someone has successfully spoofed a Web site or gained information.

Internet Explorer has a long history of security flaws, almost all of which have been patched at one time or another.

Copyright 2002 INT Media Group, Incorporated All Rights Reserved.  
[Legal Notices](#), [Licensing, Reprints, & Permissions](#), [Privacy Policy](#).  
<http://www.internet.com>

