

Please note: 3Com® Embedded Firewall defense solutions described in this chart presume that 3Com Firewall Cards are installed in vulnerable systems and can communicate with 3Com Embedded Firewall Policy Servers.

Date: March 17, 2003 Advisory CA-2003-09: Buffer Overflow in Core Microsoft Windows DLL		3Com Embedded Firewall (EFW) Solution	
		Threat Mitigation	Security Policy Details
Operating Systems	Microsoft: Windows 2000 Server / Windows 2000 Advanced Server / Windows 2000 Professional	EFW-protected IIS web servers enforce least-privileged policies that restrict access to need-to-know users only. Users or IP addresses not explicitly defined by the policies will not have access to these hosts or services. Should IIS web server become infected with malicious code, EFW provides immediate quarantine and audit response at the hardware level. This prevents internal systems from being further used as attack hop-off points into the network. Because the hardware is impervious to malicious code, and EFW effectively isolates a compromised server and any malicious code it contains. Hardware-based processing also helps maintain network quality of service. (QoS)	Hardened IIS web server policy protects hosts from e-mail or out-of-band threats and prevents them from propagating malicious code to other systems in the network. Threat attempts are logged back to the EFW policy server via real-time alerts. Policy rules: <ul style="list-style-type: none"> ▪ Restrict IIS server access to only those users with "need-to-know" rights ▪ Deny traffic from all other IP addresses ▪ Log and audit all unauthorized initiation attempts ▪ For added protection, deny packet sniffing (promiscuous mode spying) and IP spoofing (address masquerading/hiding)
Threat Condition (THREATCON)	Description: Buffer overflow vulnerability in the Win32 API libraries of Microsoft Windows 2000. High Risk! #1 in the "Top 10 Internet Security Vulnerabilities for Windows Systems" (SANS/FBI, October 2001). Exploitation: This vulnerability is being actively exploited on WebDAV-enabled IIS 5.0 servers. It allows a remote attacker to execute arbitrary code on vulnerable systems.		
Recommended Defense	<ul style="list-style-type: none"> ▪ Use the Windows Update command or download and install patch from the Microsoft website. ▪ Microsoft recommends disabling WebDAV service until a patch can be applied. For added safety, disable IIS server or restrict buffer size. 		

Date: March 11, 2003 Advisory CA-2003-08: Increased Activity Targeting Windows Shares		3Com Embedded Firewall (EFW) Solution	
		Threat Mitigation	Security Policy Details
Operating Systems	Microsoft: Windows 2000 / Windows 2000 Server / Windows 2000 Advanced Server / Windows 2000 Professional	EFW-protected remote hosts can deny access to port 445/TCP from all unauthorized IP addresses on Windows hosts. This allows usage of Windows SMB resource sharing for hosts or individuals on a need-to-know basis. Remote end systems are guarded against e-mail and other Internet-based threats, as well as prevented from propagating malicious code into the network.	Telecommuter policy for controlling access to SMB resources is easily constructed from preconfigured EFW rulesets. Threat attempts are logged back to the policy server via real-time alerts. Policy rules: <ul style="list-style-type: none"> ▪ Block ports 445/TCP from all unauthorized IP addresses (or, allow access only to IP addresses with need-to-know privileges) ▪ Block access to any host or site not explicitly defined within the policy ▪ Deny traffic from all other IP addresses ▪ Log and audit all unauthorized initiation attempts ▪ For added protection, deny packet sniffing (promiscuous mode spying) and IP spoofing (address masquerading/hiding)
Threat Condition (THREATCON)	Description: Null or weak administrator passwords in Server Message Block (SMB) file shares. High Risk! #4 in the "Top 10 Internet Security Vulnerabilities for Windows Systems" (SANS/FBI, October 2001). Exploitation: In recent weeks, thousands of residential systems have been attacked and compromised via broadband Internet access. Attackers have exploited a resource-sharing vulnerability in Windows XP and 2000—they run Server Message Block (SMB) resource shares directly on port 445/TCP, rather than running NetBIOS over TCP/IP (NBT). This makes them highly vulnerable to password-cracking tools—such as W32/Deloder, GT-bot, sdbot, and W32/Slackor. Older versions of Windows (Me, NT, and 9x) are less susceptible because SMB runs on NBT, using ports 137/TCP/UDP, 138/UDP, and 139/TCP.		
Recommended Defense	<ul style="list-style-type: none"> ▪ Use the Windows Update command or download and install patch from the Microsoft website. ▪ Microsoft recommends disabling SMB service until a patch can be applied. ▪ Restrict access to NetBIOS by blocking access to the port 445/TCP used by Windows SMB. ▪ CERT®/CC recommends using a network perimeter appliance or host-based firewall to block unauthorized backdoor access to the network. These ingress-filtering devices manage the flow of traffic as it enters the network. External hosts are granted internal connections only to public services and specified ports. Another beneficial feature is real-time alerting that notifies users or administrators when a system is compromised. 		



3Com Corporation, Corporate Headquarters, 5500 Great America Parkway, P.O. Box 58145, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Possible made practical is a trademark of 3Com Corporation. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

Please note: 3Com® Embedded Firewall defense solutions described in this chart presume that 3Com Firewall Cards are installed in vulnerable systems and can communicate with 3Com Embedded Firewall Policy Servers.

Date: February 19, 2003
Advisory CA-2003-05: Multiple Vulnerabilities in Oracle Servers; ORACLE.EXE (VU#953746), WebDAV module (VU#849993, VU#511194)

3Com Embedded Firewall (EFW) Solution

Threat Mitigation

Security Policy Details

Operating Systems
Oracle: Oracle8i Database v 8.1.7 / Oracle8 Database v 8.0.6 / Oracle9i Application Server (Release 9.0.2 and 9.0.3)
Microsoft: Windows systems running Oracle9i Database (Release 1 and 2)

Threat Condition (THREATCON)
Description: Buffer overflow vulnerability in ORACLE.EXE binary of Oracle9i Database Server.
High Risk! Vulnerability can be exploited prior to authentication.
Exploitation: An attacker can exploit this vulnerability by enticing a user to open an e-mail attachment, visit a web page, or browse to a folder containing malicious code. Once executed, the attacker can install arbitrary code to control the compromised system using the privileges of the victim.

Description: Vulnerabilities in Oracle9i Application Server modules: DAV_PUBLIC and MOD_ORADAV
High Risk! Vulnerability can be exploited prior to authentication.
Exploitation: Either vulnerability could be exploited by a malicious and knowledgeable user launching a DoS type attack to crash the system.

Description: Vulnerability in Oracle9i Application Server format string due to Apache DAV module default setting being "on."
High Risk! Vulnerability can be exploited prior to authentication.
Exploitation: Attackers can anonymously upload files to the server or exploit a format string bug in the one of the logging functions. Using the "copy" command, an attacker supplies a incompatible destination URL (different scheme or port) to initiate a "502 Bad Gateway" response. This logged format string can be then exploited to install arbitrary code.

Description: Buffer overflow vulnerability in bfilename() function (DIRECTORY parameter) of Oracle9i Database Server.
Exploitation: Requires the ability to log on to the database server with a valid user ID and password but can be executed remotely via default public account. Arbitrary code supplied by an attacker executes with the same privileges as the user running the service. The default account is typically "Oracle" on Linux/UNIX platforms and "Local System" on Windows XP/2000/NT systems. An attacker uses these default account privileges to submit an overly long DIRECTORY name to the vulnerable system, which triggers a buffer overrun in the bfilename() function. This threat can completely compromise database contents and possibly compromise the operating systems in vulnerable hosts.

Description: Buffer overflow vulnerability in TZ_OFFSET function (time zone name service) of Oracle9i Database Server
Exploitation: Requires the ability to log on to the database server with a valid user ID and password, but can be executed remotely via default public account. The default account is typically "Oracle" on Linux/UNIX platforms and "Local System" on WindowsXP/2000/NT systems. Using these default account privileges, an attacker submits a long character string to the time zone name. The attacker can then overwrite a saved return address on the stack of Oracle process. This threat can completely compromise database contents and possibly compromise the operating systems in vulnerable hosts.

Description: Oracle remote system authentication vulnerability.
Exploitation: No user ID or password is required to exploit this vulnerability. An attacker attempts to log onto a vulnerable system with an overly long user name, which can trigger a buffer overflow event as the database stack tries to overwrite the saved return address. An attacker then needs to write a specific exploit because most client applications will truncate long user names. This threat can completely compromise database contents and possibly compromise the operating systems in vulnerable hosts.

Description: Buffer overflow vulnerability in TO_TIMESTAMP_TZ function (time stamp parameter) of Oracle9i Database Server
Exploitation: Requires the ability to log on to the database server with a valid user ID and password, but can be executed remotely via default public account. The default account is typically "Oracle" on Linux/UNIX platforms and "Local System" on Windows XP/2000/NT systems. Using these default account privileges, an attacker submits a long character string to the time zone name. The attacker can then overwrite a saved return address on the stack of Oracle process. This threat can completely compromise the database contents and possibly compromise the operating system in a vulnerable host.

EFW-protected Oracle servers can enforce least-privileged policies, restricting system access to users with need-to-know rights and specified ports only. Blocking unauthorized IP addresses or personnel from Oracle services significantly reduces the risk of exposure to internal and external threats.

In addition, should an Oracle machine be successfully invaded, EFW automatically blocks all incoming/outgoing communications, effectively isolating the malicious threat from the rest of the network.

Hardened Oracle server policy allows "need-to-know" access for authorized users and services only and blocks all unauthorized access attempts.

- Policy rules:**
- Allow "need-to-know" system access on the following ports only:
 66/TCP, 1521/TCP, 1525/TCP, 1527/TCP, 1529/TCP, 1571/TCP, 1575/TCP, 1630/TCP, 1748/TCP, 1754/TCP, 1808/TCP, 1809/TCP, 1830/TCP, 2481-2484/TCP, 3339/TCP, 7771-7777/TCP, 66/UDP, 1521/UDP, 1525/UDP, 1527/UDP, 1529/UDP, 1571/UDP, 1575/UDP, 1630/UDP, 1748/UDP, 1754/UDP, 1808/UDP, 1809/UDP, 1830/UDP, 2005/UDP, and 2481-2484/UDP
 - Deny traffic from all other IP addresses
 - Log and audit all unauthorized initiation attempts
 - For added protection, deny packet sniffing (promiscuous mode spying) and IP spoofing (address masquerading/hiding)

Recommended Defense

- Disable unnecessary Oracle services until patch can be applied, if available.
- Restrict network access by running Oracle service with least privileged-user access.



3Com Corporation, Corporate Headquarters, 5500 Great America Parkway, P.O. Box 58145, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Possible made practical is a trademark of 3Com Corporation. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

Please note: 3Com® Embedded Firewall defense solutions described in this chart presume that 3Com Firewall Cards are installed in vulnerable systems and can communicate with 3Com Embedded Firewall Policy Servers.

Date: January 25, 2003 Advisory CA-2003-04: MS-SQL Server Worm; VU#484891 (CVE: CAN-2002-0649)		3Com Embedded Firewall (EFW) Solution	
		Threat Mitigation	Security Policy Details
Operating Systems	Microsoft: Any Microsoft Windows Operating System (NT/2000) running Microsoft SQL Server 2000 or Microsoft Desktop Engine (MSDE) 2000		
Threat Condition (THREATCON)	<p>Description: Self-propagating malicious code that exploits the resolution service of Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000.</p> <p>High Risk! #3 in the "Top 10 Internet Security Vulnerabilities for Windows Systems" (SANS/FBI, October 2001).</p> <p>Exploitation: Referred to as SQL Slammer, W32.Slammer, or Sapphire worm, this malicious code has caused widespread disruption in systems across the Internet. In SQL Server computers, the self-propagating malicious code exploits a stack buffer overflow vulnerability, which allows the execution of arbitrary code. The worm then uses the compromised host to craft and send malicious-code packets of 376-bytes to randomly chosen IP addresses on ports 1433/udp and 1434/udp. Propagation continues in a cascade-like chain as other vulnerable machines receiving these packets generate new worms and scan for accessible systems.</p>	<p>EFW-protected SQL servers can enforce a least privileged user-based policies that restrict users to need-to-know access only. Users will not have access to hosts or sites not explicitly defined by these policies. This prevents worms from exploiting operating system vulnerabilities, as well as prevent them from propagating across the network.</p> <p>Should an internal host be successfully infected with malicious code, EFW can provide immediate quarantine and audit response. This prevents SQL worms from propagating across the entire network by denying access at the hardware level. Because the hardware is impervious to malicious code, and EFW effectively isolates a compromised server and any malicious code it contains. Hardware-based processing also helps maintain network quality of service. (QoS)</p> <p>EFW adds two-way protection by providing defenses against threats that originate from external and internal resources.</p>	<p>Hardened SQL server policy protects hosts from e-mail or out-of-band threats and prevents them from propagating malicious code to other systems in the network. Threat attempts are logged back to the EFW policy server via real-time alerts.</p> <p>Policy rules:</p> <ul style="list-style-type: none"> ▪ Restrict system access to only those users with "need-to-know" rights ▪ Block access to any host or site not explicitly defined within the policy ▪ Deny traffic from all other IP addresses ▪ Log and audit all unauthorized initiation attempts ▪ For added protection, deny packet sniffing (promiscuous mode spying) and IP spoofing (address masquerading/hiding)
Recommended Defense	<ul style="list-style-type: none"> ▪ Use the Windows Update command or download and install patch from the Microsoft website. Microsoft recommends disabling Windows Locator service until a patch can be applied. ▪ Restrict access to NetBIOS by blocking access to the ports used by Windows Locator service—137/TCP/UDP, 138/UDP, 139/TCP, and 445/TCP. This limits system exposure to attacks from outside perimeter only. Attacks originating within the network can still exploit this vulnerability ▪ CERT®/CC recommends using a firewall product, such as a network perimeter appliance or host-based firewall. These products block unauthorized backdoor access to the network by managing the flow of traffic as it enters the network. This ingress filtering permits external hosts to initiate internal connections only to specific ports on systems that provide public services. Some of these products also can alert users or administrators when a system is compromised. 		



3Com Corporation, Corporate Headquarters, 5500 Great America Parkway, P.O. Box 58145, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Possible made practical is a trademark of 3Com Corporation. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.

Please note: 3Com® Embedded Firewall defense solutions described in this chart presume that 3Com Firewall Cards are installed in vulnerable systems and can communicate with 3Com Embedded Firewall Policy Servers.

Date: January 23, 2003 Advisory CA-2003-03: Buffer Overflow in Windows Locator/NETBios Service (SMB shares)		3Com Embedded Firewall (EFW) Solution	
		Threat Mitigation	Security Policy Details
Operating Systems	Microsoft: Windows NT 4.0 / Windows NT 4.0, Terminal Server Edition / Windows 2000 / Windows XP	EFW-protected hosts can deny access to ports 139/TCP and 445/TCP from all unauthorized IP addresses on Windows hosts. EFW can allow usage of these Windows Locator service ports for hosts or individuals on a need-to-know basis. EFW guards Windows-based hosts against exploitation, regardless of whether attackers are outside or inside the perimeter of the network.	Confidential or sensitive system policy controls access to the ports used by Windows Locator service. Policy is easily constructed using preconfigured EFW rulesets. Policy rules: <ul style="list-style-type: none"> ▪ Block Ports 445 and 139 TCP from all unauthorized IP addresses (or, allow access only to IP addresses with need-to-know privileges) ▪ Deny all other IP addresses ▪ Audit all unauthorized initiation attempts.
Threat Condition (THREATCON)	Description: Buffer overflow vulnerability in the Windows Locator service that maps logical names to network-specific names. High Risk! #4 in the "Top 10 Internet Security Vulnerabilities for Windows Systems" (SANS/FBI, October 2001). Exploitation: By sending an overly large request to the Windows Locator service, a remote attacker may be able to execute arbitrary code on a vulnerable system or cause the Windows Locator service to fail. If the compromised system is a domain server, it can be then instructed to trust the attacker's domain.		
Recommended Defense	<ul style="list-style-type: none"> ▪ Use the Windows Update command or download and install patch from the Microsoft website. ▪ Microsoft recommends disabling Windows Locator service until a patch can be applied. ▪ Restrict access to NetBIOS by blocking access to the ports used by Windows Locator service—139/TCP and 445/TCP. This limits system exposure to attacks from outside perimeter only. Attacks originating within the network can still exploit this vulnerability. 		

Date: December 19, 2002 Advisory CA-2002-37: Buffer Overflow in Microsoft Windows Shell Microsoft Security Bulletin: MS02-072 (CVE: CAN-2002-1327)		3Com Embedded Firewall (EFW) Solution	
		Threat Mitigation	Security Policy Details
Operating Systems	Microsoft: Windows XP / Windows XP Home Edition / Windows XP Professional / Windows XP Tablet PC Edition / Windows XP Media Center Edition	EFW-protected hosts can enforce least privileged user-based policies that restrict users to need-to-know access rights only. Users will not have access to hosts or sites not explicitly defined by these policies. EFW prevents attackers from invading remote systems, as well as prevent them from being exploited to launch malicious audio or multimedia code. Should a host be successfully invaded, EFW automatically blocks all incoming/outgoing communications, effectively isolating the malicious threat from the rest of the network.	Least-privileged user policy provides two-way protection by denying malicious access to EFW-protected hosts, as well as keeping them from being used to propagate malicious code to other systems in the network. Policy rules: <ul style="list-style-type: none"> ▪ Restrict system access to only those users with "need-to-know" rights ▪ Block access to any host or site not explicitly defined within the policy ▪ Deny traffic from all other IP addresses ▪ Log and audit all unauthorized initiation attempts ▪ For added protection, include a rule that denies "packet sniffing" (promiscuous mode spying) and "IP spoofing" (IP masquerading/hiding)
Threat Condition (THREATCON)	Description: Buffer overflow vulnerability in Microsoft Windows shell. High Risk! #4 in the "Top 10 Internet Security Vulnerabilities for Windows Systems" (SANS/FBI, October 2001). Exploitation: An attacker entices a user to execute a malicious *.MP3 or *.WMA file by having them open an e-mail attachment, visit a web page, or browse to a folder containing the malicious code. The attacker can then execute arbitrary code using the operating system privileges of the victim.		
Recommended Defense	<ul style="list-style-type: none"> ▪ Use the Windows Update command or download and install patch from the Microsoft website. 		



3Com Corporation, Corporate Headquarters, 5500 Great America Parkway, P.O. Box 58145, Santa Clara, CA 95052-8145

To learn more about 3Com solutions, visit www.3com.com. 3Com is publicly traded on NASDAQ under the symbol COMS.

Copyright © 2003 3Com Corporation. All rights reserved. 3Com and the 3Com logo are registered trademarks of 3Com Corporation. Possible made practical is a trademark of 3Com Corporation. CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University. All other company and product names may be trademarks of their respective companies. While every effort is made to ensure the information given is accurate, 3Com does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice.