Global Information Assurance Certification Paper

SANS/GIAC Practical Assignment

For GCIH Certification

Version 2.1

SECURITY BREACH; CODE RED

BY

ROGER T. ZEHNER

Table of Contents

1. Preface

The following is a current case being addressed at company XYZ. I have changed the name of the company, as well as anything that may identify the company. Law enforcement has been included in this investigation.

This issue is being addressed by the FBI, which was called in for further forensics on the servers. The FBI currently has the hard drives in their possession.

2. Executive Summary

Company '***XYZ'*** has a contract with Company '***ABC'*** to perform a vulnerability assessment on their environment. On March 21, 2002, Company ABC found an entrance into company XYZ's web network. Based on the initial information and subsequent research, it was determined that the security breach had originally occurred in November of 2001 and the last time the point of entry was used was March 13, 2002.

Through internal investigation, it was determined that the entrance was a NT server running 4.0 with IIS 5.0 in the Quality Assurance (QA) environment. It was determined that the cause of entrance was back level NT operating system software and back level security patches.

Since this was the QA environment and no sensitive information is allowed in this environment per policy, no information was stolen. The 2 NT servers that were compromised were immediately removed from the network.

The attack seemed to use the framework of the Code Red Worm to expose the IIS 5.0 vulnerability on NT 4.0 servers and then used the UPLOAD.ASP to upload content to the web server.

3. The Exploit

The attacker(s) utilized the "Code Red" worm against the servers to exploit the vulnerability in IIS. From there, they utilized the command line, called from the web server, to perform other operations. The CVE# is shown in **Appendix 7.**

- CVE-2001-0500
  - http://online.securityfocus.com/bid/2880
  - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2001-0500

3.1. Exploit Name and Description

The exploit used to find the vulnerability was Code Red using a port scan product such as, NMAP or Nessus. The Code Red worm exposes any server running IIS 4.0, 5.0, 6.0 and IIS servers running Outlook Web Access. The Microsoft security patch that prevents the Code Red worm from infecting the NT servers is 300972. The advisory is shown in **Appendix 3**.

3.2. Operating System

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed.
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed.
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager running IIS.
- Unpatched Cisco 600 series DSL routers.

3.2.1. Protocols/Services/Applications

Servers running IIS 4.0, 5.0, 6.0 and IIS servers running Outlook Web Access through TCP port 80.

IIS is Internet Information Server (IIS) and is a World Wide Web server, a Gopher server and an FTP server all rolled into one. IIS means that you can publish WWW pages and extend into the realm of ASP (Active Server Pages) whereby JAVA or VBscript (server side scripts) can generate the pages on the fly. IIS has fun things like application development environment (FrontPage), integrated full-text searching (Index Server), multimedia streaming (NetShow), and site management extensions.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is actually a collection of protocols, or rules, that govern the way data travels from one machine to another across networks.

3.2.2. Brief Description

The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow. The worm spreads from one IIS server to another. No intermediate hosts or applications are required. The

worm exploits the buffer overflow in idq.dll, launching from memory numerous attacks against random IP addresses in an attempt to infect other servers. The process in memory returns static content in response to any page request from the compromised server, appearing to deface the web page and leaving a link to worm.com. However, it appears that a search for this static content, for example worm.com, will not yield any results from disk, as the information seems to reside solely in memory.

Rebooting an affected web server, should eliminate the worm, however, any unpatched system is likely to be re-infected by other compromised IIS servers. In addition, the web, ftp, and SMTP services of IIS may be halted. Even that however, will not expose any back doors that were opened if the attacker added other vulnerabilities to the Code Red code.

A worm is a program that makes copies of itself to allow it to infect other computers, for example from one disk drive to another, or by copying itself using email or some other transport mechanism. It may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort and does not require a user to execute.

3.2.3. Variants

The different Code Red variants (aliases): Code Red II, CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C.

3.2.3.1. Code Red II, CodeRed.v3, CodeRed.C, CodeRed III, W32.Bady.C

The reason why these viruses have been called a variant of the original Code Red is because they use the same "buffer overflow" exploit to propagate to other Web servers. These variants have a different payload which allows the hacker to have full remote access to the Web server.

The version that has gotten all this attention was supposed to infiltrate vulnerable computers, use them to replicate itself and then causes a Denial of Service attack.

There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victim system.

4. The Attack

4.1. Description and Diagram of Network

The Web environment for company XYZ is configured such that the routers are being used to filter incoming traffic. The filters are set up to only allow incoming traffic to ports 80 and 443. This has the effect of blocking external addresses from attaching to company XYZ's Web servers using anything but normal web and secure web traffic. This seems to be adequate security when considering that company XYZ has a good security policy surrounding their Web server configuration, and they employ state of the art Intrusion Detection software to alert in case of an attack. The network diagram can be seen in **Appendix 1**.

Company XYZ is not using a firewall, but are being used for packet-filtering at the router and only allowing traffic from port 80 and 443.

The type of router that is used at company XYZ is Cisco 7513. The IOS version is 11.1. Company XYZ runs two Cisco routers for redundancy purposes (incase one fails the other will stand in).

The Cisco 7513 router supports multiprotocol, multimedia routing and bridging with a wide variety of protocols and any combination of available electrical interfaces and media. Network interfaces reside on interface processors that provide a direct connection between the two CyBuses in the Cisco 7513 and your external networks. The Cisco 7513 has thirteen slots: interface processor slots 0 through 5, Route Switch Processor (RSP2 or RSP4) slots 6 and 7, and interface processor slots 8 through 12.

4.2. Protocol Description

TCP/IP, HTTP were used. TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is actually a collection of protocols, or rules, that govern the way data travels from one machine to another across networks.

HTTP is a client-server protocol by which two machines can communicate over a tcp/ip connection. An HTTP server is a program that sits listening on a machine's port for HTTP requests. An HTTP client opens a tcp/ip connection to the server via a socket, transmits a request for a document, then waits for a reply from the server. Once the request-reply sequence is completed, the socket is closed. So the HTTP protocol is a transactional one. The lifetime of a connection corresponds to a single request-reply sequence. (a transaction)

4.3. How the Exploit Works

As part of its installation process, IIS installs several ISAPI extensions -- .dlls that provide extended functionality. Among these is idq.dll, which is a component of Index Server (known in Windows 2000 as Indexing Service) and provides support for administrative scripts (.ida files) and Internet Data Queries (.idq files).

Security vulnerability results because idq.dll contains an unchecked buffer in a section of code that handles input URLs. An attacker who could establish a web session with a server on which idq.dll is installed could conduct a buffer overrun attack and execute code on the web server. Idq.dll runs in the System context, so exploiting the vulnerability would give the attacker complete control of the server and allow him to take any desired action on it.

The buffer overrun occurs before any indexing functionality is requested. As a result, even though idq.dll is a component of Index Server/Indexing Service, the service would not need to be running in order for an attacker to exploit the vulnerability. As long as the script mapping for .idq or .ida files were present, and the attacker were able to establish a web session, he could exploit the vulnerability.

4.4. Description and diagram of the attack

The attacker probably used NMAP or Nessus to run a port scan against the servers to see what was vulnerable to Code Red. Because Company XYZ allows port 80 traffic in to the web environment; the attacker was able to get to a QA web server running NT 4.0 with IIS 5.0 service running. Once the attacker gained access to the Web Server, the attacker used a SQL Injection to snoop the Database Servers to try and reach critical data. To view the Network diagram of the attack, see **Appendix 6**.

4.5. Signature of the Attack

The "Code Red" worm activity can be identified on a machine by the presence of the following string in a web server log file:

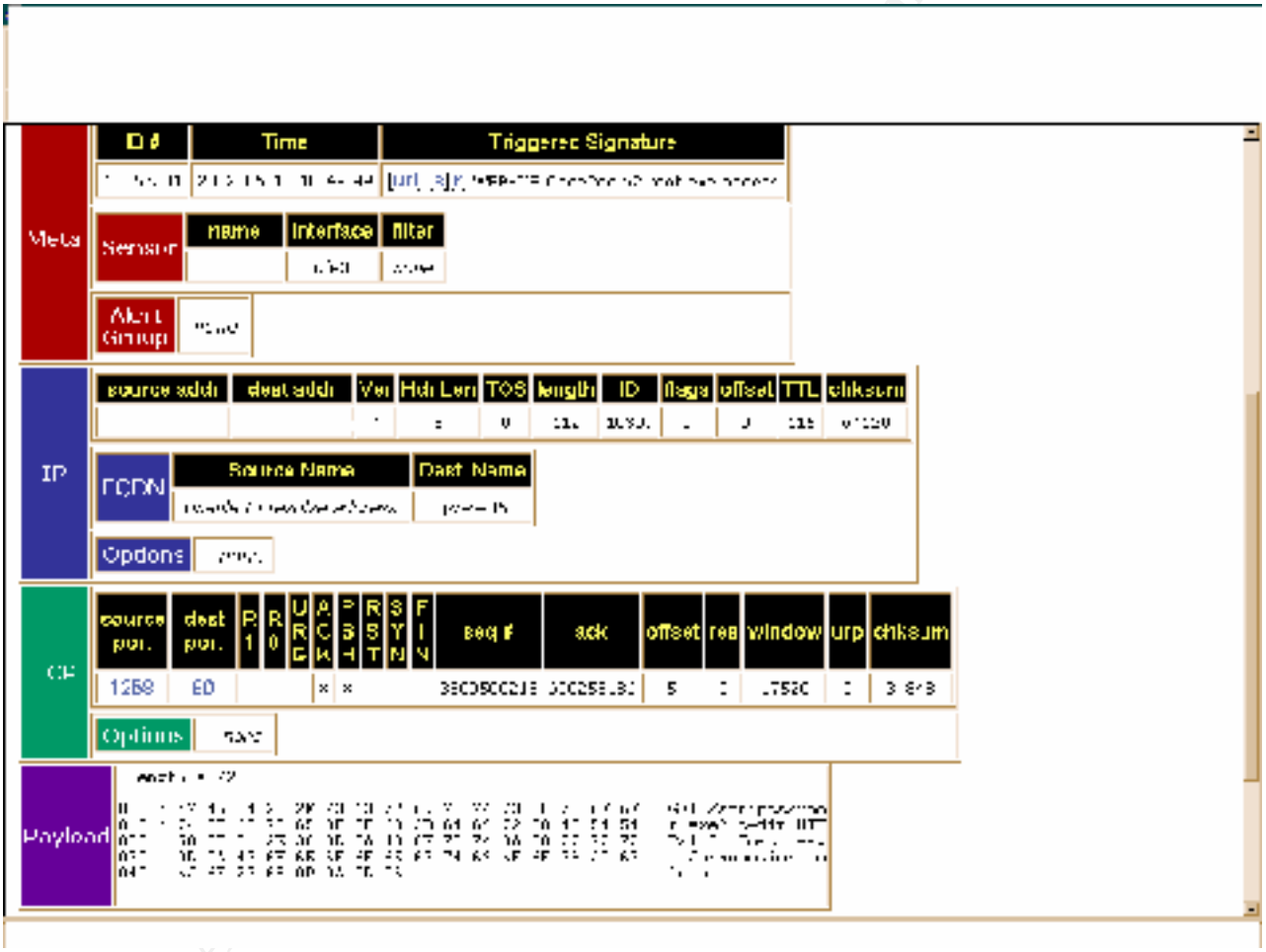
GET /default.ida?
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNu9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0
003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403

The presence of this string in a log file does not necessarily indicate compromise. Rather it only implies that a "Code Red" worm attempted to infect the machine.

Additionally, web pages on victim machines may be defaced with the following message:

HELLO! Welcome to http://www.worm.com! Hacked By Chinese!

Company XYZ was not using Snort at the time of the incident, but here is a recent snap shot of Snort capturing Code Red.



4.6. *How to Protect Against it*

The other issue company XYZ needs to address is to make sure all servers are up to current OS levels and security patch levels. One should also make sure that if IIS is not needed the service should not be started. Monitor incoming Snort messages and alerts.

A firewall being installed at company XYZ might be an appropriate step in this case. The idea behind the firewall in the web environment is two-fold. The primary purpose is to only allow traffic that should be allowed. For instance, in company XYZ's web environment they need external IP addresses to be able to access their web servers on port 80 and 443. It seems they have that now, with the exception of IP spoofing. A firewall can block the hacker attempting to spoof one of the internal addresses. Some firewalls can even do content filtering. That means they can look for particular well-known attacks and block them before they even enter their web environment. The network diagram in **Appendix 2** would offer a better security set-up for company XYZ.

Other problems that can be solved using a firewall in company XYZ's environment is; if a hacker was able to gain access to a web server he/she would have to go back through the firewall in order to gain access to any internal resources. The firewall configuration would allow only very restricted communication between the web servers and application servers. Therefore, attempts to gain access via conventional communication ports would be blocked by the firewall.

Another benefit of some firewalls is the ability to monitor connection state, which prevents some specially crafted packets from slipping through.

There are many different firewall solutions on the market with different benefits to each. The end result along with the current security methods within the web environment would be increased security.

Snort, which is a network intrusion detection system/packet capturer/logger, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. With the use of Snort, you can be flexible with the rules to describe traffic that it should collect or pass, as well as a detection engine. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a WinPopup message to Windows clients using Samba's smbclient.

4.6.1. What can someone running the vulnerability do so his or her system wouldn't be compromised?

Make sure that all your servers are up to current system operating levels and you have the current security patch level. Disabling IIS if not needed would be a wise choice, also.

Someone running the vulnerable system should first verify that a firewall is being used. Make sure that the firewall is configured according to the vendor's specifications.

It would also be beneficial to have current back ups performed on all your servers.

A person also may want to do research on some software products that may also help, such as Snort, Tripwire, etc… These products, if configured properly, could be used to review logs and determine if anyone is trying to get into your network.

4.6.2. What could or should the vendor do to fix the vulnerability?

There is this image that goes with a company when they can get a product "to market" first. With more testing and less emphasis on trying to get a new product out to market first, a lot of these vulnerabilities could/might be prevented.

I am a big believer in testing something. Besides making sure it does what the client wants, it also might protect the client from someone exposing vulnerabilities in the product.

5. The Incident Handling Process

5.1. Preparation

The most important document that any company needs is an attack policy. Procedures on what to do when someone hacks into their network. Fortunately, company XYZ has an up-to-date document outlining what the processes are to follow, as well as contact information.

Also, It would be in the best interest to the company if everyone on the incident response team were certified in incident handling. Some good certifications that are available are listed below:

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- TruSecure ICSA Certified Security Associate (TICSA)
- CISCO Certifications
- Certified Computer Crime Investigator (Basic and Advanced) (CCCI)
- Certified Computer Forensic Technician (Basic and Advanced) (CCFT)
- Certified Forensic Computer Examiner (CFCE)
- GIAC Certifications (Global Information Assurance Certification)

5.1.1. List of policies that company XYZ has in place

- **Monitoring, Alert Identification and Initial Notification**
- **Incident Triage and Team Activation**
  - Alerts
    - *Red Alerts*
      - ⇒ An event that is or could become a serious and immediate threat (actual or potential penetration or

denial of service) to any networks, routers, servers, firewalls, network management hosts or attached LANs, or user hosts.

⇒ A security incident is known to the public or may become known to the public.

⇒ Identified active or inactive intrusions.

⇒ Incidents where individuals claim to have penetrated XYZ's networks.

⇒ Recently publicized vulnerabilities that involve current utilized devices or software.

➢ *Yellow Alerts*

⇒ An event, which is, or could become, a future threat, but which has been determined as not a serious and/or immediate threat.

⇒ Repeated activity directed against XYZ detected by NetRanger.

⇒ Vulnerabilities discovered through internal testing that cannot be exploited directly on the affected host from the Internet.

➢ *Blue Alerts*

⇒ An event that is, or could become, a minor annoyance or threat, or has been determined as a non-threat situation resulting from either authorized or unauthorized network activity.

⇒ Vulnerabilities that involve advisories for theoretical exploits, but have yet to be proven.

❑ **Initial Assessment**

- Assess Risk

  Review Network Mapping to determine:

  ⇒ Hardware/software to include security resources/audit/alarms

  ⇒ Connectivity, IP addressing scheme

  ⇒ SysAdmins, Security Admin, name, contact number, delegate

⇒ Operational descriptions of the data/processes

⇒ Criticality of data/process

⇒ Vulnerability status: last known assessment

⇒ What is the Maximum Tolerable Downtime (MTD) for the given system

⇒ Is the compromised machine critical

⇒ If a critical determination cannot be made what impact would taking machine off-line have

⇒ Do any critical machines "trust" the compromised machine

⇒ Are any critical machines on the same subnet as the compromised machine

⇒ Do any critical machines trust a machine on the same subnet as the compromised machine

⇒ Does sensitive information travel by the compromised machine

- Review Logs

  ⇒ Firewalls

  ⇒ Routers

  ⇒ Remote access servers

  ⇒ Web servers

  ⇒ DSS

  ⇒ Other network devices

  ⇒ Identify traffic matching attacker profile from source/destination address of compromised machine or suspected hacker

  ⇒ Identify traffic matching suspected compromise method

- Formulate Recovery Options

  ⇒ Determine the consequence of each recovery action

  ⇒ Core Team presents options

⇒ Two or three most viable options are selected, list the pros and cons of each

⇒ Meet with management.

- **Management Review Options**
  - Establish War Room/Conference Call Number
  - Network and System Recovery Options
    - ⇒ Identify the source of the attack and correct vulnerabilities if known
    - ⇒ Remove system from network to stop the attack
    - ⇒ Recovery time for each portion from simple analysis to complete computer forensic evidence gathering
    - ⇒ The level of assurance available depending on the recovery option chosen
    - ⇒ The level of effort that will be required of client system and network administrators
    - ⇒ User impact
    - ⇒ Business impact
    - ⇒ Prerequisites to options (such as warning banners for successful prosecution)
    - ⇒ Discuss tradeoff between capture of computer forensic data vs. business interruption/resumption
  - Red Alert Hacker Scenarios
    - ⇒ Management must also be prepared to implement recovery options dealing with the individual responsible for the intrusion
- **Incident Recovery**
  - Investigate
    - ⇒ Review logs from impacted environment
    - ⇒ If restorative Response Team will do the forensics
    - ⇒ If criminal, Response Team will take over the gathering of evidence

⇒ Perform computer forensics mirroring of affected hosts and systems

⇒ Maintain original evidence through a designated evidence custodian

⇒ Investigate mirrored image

⇒ Perform port scans

⇒ Use host and network vulnerability analysis tools (beware, these actions are noisy and will alert an active hacker.)

⇒ Crack the passwords of the compromised machine to compare to other system accounts/passwords to other systems

⇒ Check other systems of similar operating system/vulnerability additional levels of compromise

⇒ Test physical access/network access via internal sniffers, check wiring closets

- Isolate and Contain

⇒ Disconnect compromised computer from network

⇒ Isolate computer from broadcast domain

⇒ Introduce host based access controls

⇒ Use packet filtering at network boundaries

⇒ Use connection hijacking tools to hijack or kill the session from an intruder

⇒ Limit dial-in access

⇒ "Fishbowl" the intruder into an area that appears normal (isolated from the network) to gather evidence

- Rebuild and Reactivate

⇒ Change passwords, host-wide, system- wide, or enterprise-wide

⇒ Secure vulnerabilities for machines not directly compromised, by turning off unused services, applying operating system and application patches, strong passwords, and competent administration.

Check operating system-specific security checklists for the appropriate actions.

⇒ Restore from backups (if backups were not compromised) and secure

⇒ Rebuild from CD-ROM, then secure

⇒ Introduce other countermeasures such as host-based controls, packet filters, firewalls, intrusion detection, user education, policy, etc. Rather than attempt to add these countermeasures during an incident response mission, they should probably be listed in the final report as recommended further action.

⇒ Provide user education and create additional policy if compromise was due to a policy breach

- **Incident Closure**

  - Review

    ⇒ Complete project team performance reviews

    ⇒ Review incident performance

    ⇒ Evaluate methodology and tool use task analysis

    ⇒ Solicit project feedback

  - Prepare and Write up Incident

    ⇒ Restoration report, limited to those with need to know, Executive Team, Core Team, Escalation contacts

    ⇒ A second investigation report may be necessary for criminal intent. It would include details for a forensic investigation that may then be used for a criminal trial. Corporate Security controls distribution.

  - Identify Areas for follow-up Review

  - Process Improvements

5.1.2. List of Tools used by Company XYZ Response Team

- **Incident Procedure Document**
- **Local Police and FBI personnel**
- **Drive Mirroring**
- **Access to back ups**
- **Snort**
- **NetRanger**
- **Sniffers**

Overall, this situation began as a very intense situation with a lot of unknowns. The teamwork, from all groups involved, that began on Friday March 21, 2002 and continued through the next twelve days was phenomenal. The application development groups and operations teams were very cooperative and assisted in any way they could. This allowed for the response team to identify root cause, gaps found in the environment and the solutions to close the gaps very quickly.

5.2. Identification

The original attack occurred in November of 2001, but was not discovered until March 21, 2002 when company XYZ contracted company ABC to do a Vulnerability Assessment. The conclusion for identifying November as the original attack time was due to the log files missing for that month, as well as some files and folders that were created about that time. It is believed that the attacker used a port scan and found the systems vulnerable to Code Red. Further research uncovered a root.exe cmd on the infected servers. Root.exe is a program left behind on IIS servers, which has been hacked as a back-door. It allows literally anyone connected to the Internet to execute any command or access any data on the machine with full priviledge.

The hacker used the two NT servers in the Quality Assurance environment as gateways into the network. Once the breach was identified, the servers were then immediately removed from the network.

In the process of reviewing the logs and the servers, it was determined that this attack could have been prevented. The servers were not up to the current OS

level, as well as the current security patch level. The hacker(s) used the framework from the Code Red worm to exploit the vulnerability in the IIS servers on the NT4.0 server. They then used the *UPLOAD.ASP* vulnerability to get to the systems.

It was determined that that the attacker may have come in from (Web site.com), which has a routable IP address, making it accessible from an external source.

There was a file, *UPLOAD.ASP* loaded on the two NT servers with the date of November and created by an account that was not there before the November date, according to log files. The file UPLOAD.ASP is not part of the standard build for these servers, so it was determined that the attacker(s) used this to execute commands on the compromised machines and send the display back to them.

The FBI was contacted and arrived at company XYZ's facilities around 1am on March 22, 2002. The FBI then began gathering documentation from the "single point of contact" person assigned to the Response Team. After the FBI gathered all documentation, they performed interviews with employees on duty working the issue.

5.3. Containment

5.3.1.1. Steps taken to contain the situation:

A Service Restoration Conference Call was convened immediately, with all of the appropriate parties. This Conference Call was moved to a more secure phone number and continued at regular intervals throughout the weekend. Daily status call began on Monday March 25th and continued until April 2nd.

The two servers identified as those as being compromised, were taken out of server rotation (network cables pulled) within 2 hours after the initial discovery of the intrusion.

The Internet Protocol (IP) addresses that were identified as where the breaches came from were "shunned" to eliminate any future access via those IP addresses. One or two of these addresses were from a XYZ

customer location. The customer(s) were notified that there is the possibility that their security might have been also breached.

The command on the router to block a single IP addresses is:

access-list 101 deny ip 10.10.10.240 0.0.0.0 any log

The command on the router to deny a whole subnet is:

access-list 101 deny ip 10.10.10.1 0.0.0.255 any log

When shunning from NetRanger it is done by right clicking on the alert and left click on shun button.

The response teams completed hands on investigations to determine when the breach occurred and if any servers other than those running the NT Operating System software were impacted.

The incident response team does not have a "jump bag" so to say. The engineering group supplied the Binaries on CD's. The incident response team had access to backup media, Ghost, call list with phone numbers and cell phones. Dual OS laptops are what Company XYZ runs on a regular basis consisting of Red Hat LINUX 7.1 and Windows 2000.

Hands on research continued through Saturday to identify if any other servers in any other environments were compromised.

The FBI was contacted and was on-site by early Saturday morning (1am) March 23rd. The FBI could not copy the information they required and determined that the servers needed to be shipped to their office, which was completed March 29th. Company XYZ made a backup copy of the disk prior to shipping and is now waiting for a reply from the FBI with their findings.

The two QA servers were shipped to the FBI and the process to put new servers in thier place will be the first week of April or when the new hardware arrives on-site.

5.4. Eradication

This is the removal of the problem. As mentioned above, the servers were removed from the network and sent to the FBI. The new hardware is in the process of being configured and restored back into server rotation.

Company XYZ identified that the cause of the incident was not having the server up to current OS level and failure to apply security patches.

Company XYZ is currently in the process of upgrading all servers to current OS and updating all security patches. Company XYZ proceeded to go out to all local servers on all domains and change every administrator password. They then went through the process of contacting every group to verify every id on the servers and remove those that no longer were being used.

The Producation, QA and development NT environments were scanned to determine if they had been compromised. The NT servers were scanned for current Operating System level, maintenance levels, and security patch levels. A list of all the servers with there OS level and security patch level; as well as the reason why they were below current company XYZ Standards were sent to the response team.

A plan was created to close the network entrance to all QA and Development servers in company XYZ's environment. The expected completion for this plan will be the last week of April. A notification is being sent to all Development teams concerning their responsibilities. With completion of this plan, the QA and Development servers will only be available through company XYZ's Intranet network, they will no longer be available through the Internet.

Research into the possible impacts of the breach will continue until the time when all servers have been examined and brought up to the current OS and security patch level.

5.5. Recovery

The servers were removed and shipped to the FBI. Company XYZ did not send just the hard drives, because the FBI did not have a system to support the raid configuration. The new servers are currently being configured to replace them. The new servers will be at the correct OS level, as well as the current security

patch level. Company XYZ is also rerunning vulnerability assessments against all servers.

Due to these servers being in the QA environment, these servers were not backed up. There is a standard image used on CD that will be used to rebuild the servers.

The product SNORT was installed on the network to identify possible security breaches and monitor for future attempts to get into the network. This product will work in conjunction with NetRanger.

A plan was developed to bring the NT servers up to the current operating system service pack level, SP6a and the current security patch level. The updates to the development servers will begin the first week of April, with QA and Production following. Penetration/vulnerability testing will continue by company ABC.

It will be important for all groups within company XYZ to monitor their systems and networks very closely for the next few months to determine that no back door was installed on any server and went undetected by the analysis performed on all machines.

5.6. Follow Up/Lessons Learned

There are several steps needed to close all the gaps.

- Implement the appropriate operating system upgrades and security patches in all environments. Company XYZ is currently doing a scan across the network to see what OS level servers are at, as well as what patch level they are at.

- Complete the plan to eliminate Internet access to the QA and Development environment servers. Company XYZ is disabling any services that are not required within the DEV and QA environments.

- Complete the review of all the operating system files and F: drive files that have changed since the week of March 13th, which is when the last entrance to the company XYZ's network by the intruder.

- Complete the replacement of the two web servers sent to the FBI.

- Change the passwords used for the QA and Development environments, since the SAMS file looks to have been uploaded.

- Determine what process changes have to be implemented as a result of the two servers that were compromised. Such as, updating the Security policy, Incident Response document and re-defining team members.

- Implemented SNORT.

- Revised Security policy based on discovered gaps in the incident response document.

- Company XYZ is implementing VTA's on a monthly basis.

- The management team has agreed to allow the incident response team to receive more training and hire more employees that are certified in incident handling.

- The response team is to continue regular status meetings until all gaps have been closed.

5.7. Conclusion

In conclusion, company XYZ learned a valuable lesson. This lesson is that at all times your OS and Security patch levels must be up to current standards. It only takes one server to be below that level to be exploited by any known attacks. In this case, this could have been avoided. The initial break in could have been avoided if the server was at the current security patch level. The second part of this was done using an older known method, which could have been avoided if the OS was at current level.

In a recent newspaper article, it stated that 90% of all hacks go unreported. It is very important that all attacks are reported to law enforcement. Yes, you might have been able to isolate and contain this problem, but the hacker is still out there causing headaches for other Security Administrators.

What makes you think that this hacker will not be back knocking at your door again?

It is also very important for security administrators to stay on top of current viruses and technologies. Keeping up-to-date with exploits and testing of new vulnerabilities will help you and your company feel better about your environment.

With this incident, I believe it opened some eyes as to how vulnerable company XYZ can be.

6. Resources

- **Mcafee Website**

http://hq.mcafeeasap.com/vulnerabilities/vuln_data/10000.asp#10088

- **CERT Website**

  http://www.cert.org/advisories/CA-2001-19.html

- **Microsoft Bulletins**

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-044.asp

- **Symantec Website**

  http://www.sarc.com/avcenter/venc/data/codered.ii.html

- **Trusecure Website**

  http://www.trusecure.com/html/tspub/hypeorhot/rxalerts/tsa01020_cid115.shtml

- **Security Focus Website**

  http://online.securityfocus.com/bid/2880

- **Aastarnet Website**

  http://www.azstarnet.com/

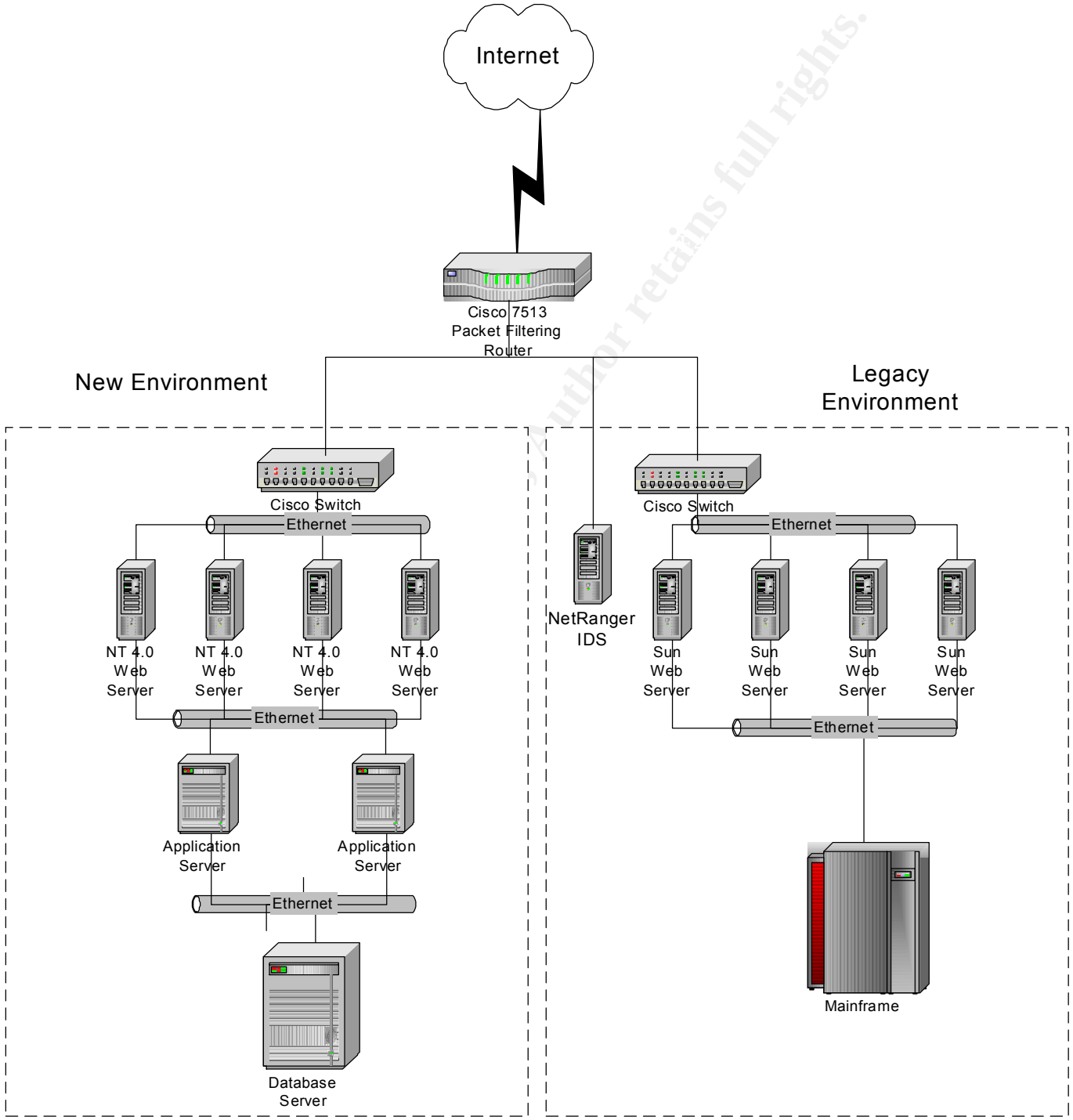
- **CVE Website**

  http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2001-0500

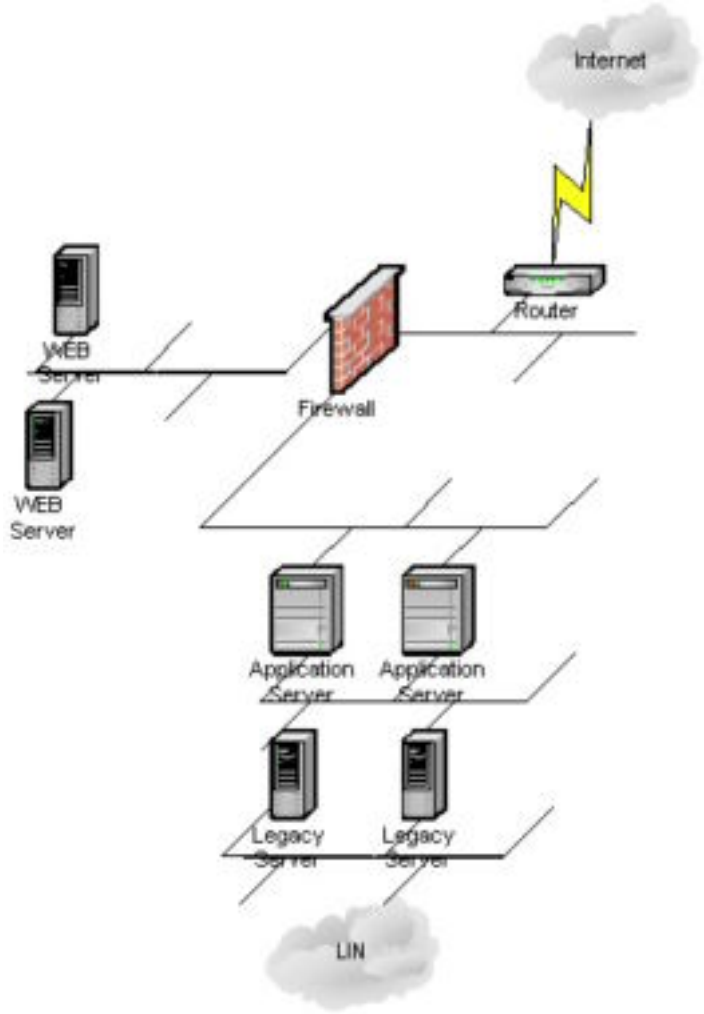
- **Antivirus Website**

  http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=CODERED.C

7. Appendix 1 – Current Network Diagram



8. Appendix 2 – More acceptable network diagram



9. Appenix 3 - CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Original release date: July 19, 2001
Last revised: January 17, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed

Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed

Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)

Unpatched Cisco 600 series DSL routers

Overview

The CERT/CC has received reports of new self-propagating malicious code that exploits IIS-enabled systems susceptible to the vulnerability described in CERT advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Other systems not directly vulnerable to this exploit may also be impacted. Reports indicate that two variants of the "Code Red" worm may have already affected more than 250,000 hosts.

10. Appendix 4 – NetRanger Log Files for Code Red

ID < Signature > < Timestamp > < Source
Address > < Dest.
Address > < Layer 4
Proto >

#0-(110-2138707) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3349
123.345.567.789:80 TCP

#1-(110-2138711) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3384
123.345.567.789:80 TCP

#2-(110-2138712) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3391
123.345.567.789:80 TCP

#3-(110-2138713) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3398
123.345.567.789:80 TCP

#4-(110-2138714) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3409
123.345.567.789:80 TCP

#5-(110-2138715) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3421
123.345.567.789:80 TCP

#6-(110-2138716) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3435
123.345.567.789:80 TCP

#7-(110-2138717) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3450
123.345.567.789:80 TCP

#8-(110-2138718) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:28:28 123.345.567.789:3473

123.345.567.789:80 TCP
#9-(110-2138726) NRS 3215/IIS DOT DOT EXECUTE Attack
2002-02-22 00:29:29 123.345.567.789:1177
123.345.567.789:80 TCP
#10-(110-2138727) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:29:29 123.345.567.789:1225
123.345.567.789:80 TCP
#11-(110-2138728) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:29:29 123.345.567.789:1272
123.345.567.789:80 TCP
#12-(110-2138729) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:29:29 123.345.567.789:1288
123.345.567.789:80 TCP
#13-(110-2138753) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:32:32 123.345.567.789:3157
123.345.567.789:80 TCP
#14-(110-2138756) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:32:32 123.345.567.789:3339
123.345.567.789:80 TCP
#15-(110-2138757) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:32:32 123.345.567.789:3440
123.345.567.789:80 TCP
#16-(110-2138758) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:32:32 123.345.567.789:3487
123.345.567.789:80 TCP
#17-(110-2138759) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:32:32 123.345.567.789:3633
123.345.567.789:80 TCP
#18-(110-2138790) NRS 3215/IIS DOT DOT EXECUTE
Attack 2002-02-22 00:37:37 123.345.567.789:2424
123.345.567.789:80 TCP

11. Appendix 5 – Microsoft Bulletin MS01-033

Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise

Originally posted: *June 18, 2001*

Summary

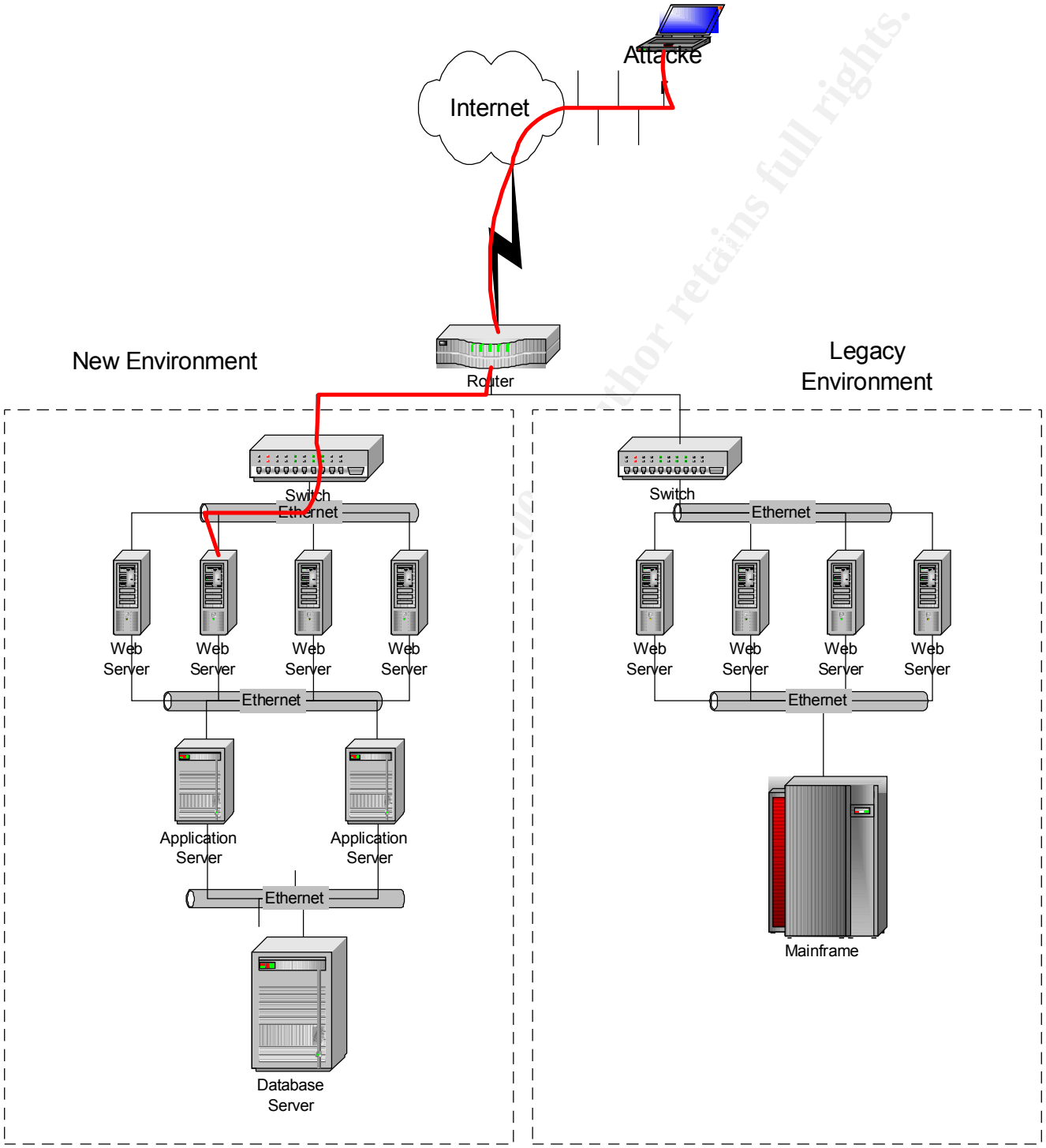
Who should read this bulletin: System administrators of web servers using Microsoft® Windows NT® 4.0 or Windows® 2000.
Impact of vulnerability: Run code of attacker's choice.
Recommendation: Microsoft strongly urges all web server administrators to apply the patch immediately.

Affected Software:

Microsoft Index Server 2.0

Indexing Service in Windows 2000

12. Appendix 6 – Network Diagram of Attack



13. Appendix 7 CVE-2001-0500

CVE Version: 20020309

This is an entry on the CVE list, which standardizes names for security problems. It was reviewed and accepted by the CVE Editorial Board before it was added to CVE.

Name	CVE-2001-0500
Description	Buffer overflow in ISAPI extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by Code Red.

References

BUGTRAQ:20010618 All versions of Microsoft Internet Information Services, Remote buffer overflow (SYSTEM Level Access)
MS:MS01-033
CERT:CA-2001-13
BID:2880
XF:iis-isapi-idq-bo(6705)
CIAC:L-098

14. Appendix 8 - Microsoft Bulletin MS01-044

15 August 2001 Cumulative Patch for IIS

Originally posted: *15 August 2001*

Summary

Who should read this bulletin: System administrators using Microsoft® Windows NT® 4.0 or Windows® 2000 web servers

Impact of vulnerability: Five vulnerabilities resulting in privilege elevation and/or denial of service

Recommendation: System administrators should apply the patch to all machines running IIS 4.0 or 5.0 immediately

Affected Software:

Microsoft Internet Information Server 4.0

Microsoft Internet Information Server 5.0

Last Updated: July 25th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Community SANS Columbia SEC504	Columbia, MD	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event
Mentor Session - SEC504	Boston, MA	Sep 26, 2017 - Nov 07, 2017	Mentor
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session AW - SEC504	Houston, TX	Oct 02, 2017 - Dec 11, 2017	Mentor
Mentor Session - SEC504	Columbia, SC	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
Community SANS Chicago SEC504	Chicago, IL	Oct 09, 2017 - Oct 14, 2017	Community SANS