Network Vulnerability Assessment Report

Sorted by IP

05/13/2005

This report lists the vulnerabilities detected by Internet Scanner after scanning the network.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
P**urpose:** For each host, the report provides the IP address, the DNS name, the operating system type, and remedy information for vulnerabilities detected by Internet Scanner.
Related reports: For a brief list of the types of vulnerabilities detected on each host, see the Line Management/Vulnerability Assessment reports.

Vulnerability Severity: H High M Medium L Low

Session Information

Session Name:	Carige[L5 webserver]	**File Name:**	Carige[2]_20050513_125501.log
Policy:	Copy of L5 Web Server	**License:**	758E24DD-D246-03C7-5483-98454C3C99F2/27 041501
Hosts Specified:	1	**Hosts Scanned:**	1
Scan Start:	13/05/2005 12.54.59	**Scan End:**	13/05/2005 13.14.06
Comment:			

IP Address {DNS Name}	Operating System
213.156.59.251 {ip-pub.fastwebnet.it}	Windows 2000

Admin Access:

No

M **HttpTraceEnabled: HTTP TRACE is enabled**

Additional Information *More Information*

port=80

HTTP TRACE support is enabled on the Web server. The HTTP TRACE method as described in RFC 2616 of the HTTP 1.1 standard is typically used for debugging and network analysis purposes to request the contents of HTTP request messages received by the Web server. On Web servers with HTTP TRACE support enabled, a remote attacker could leverage this functionality with known cross-site scripting and other Web browser vulnerabilities to obtain sensitive information about the Web server, including server cookies and authentication information. This information could then be used by the attacker to launch further attacks against the affected Web server.

Remedy:

Administrators should disable HTTP TRACE support on the Web server. HTTP TRACE support can be disabled on Apache HTTP Server using the mod_rewrite module and on Microsoft Internet Information Services (IIS) using the URLScan tool.

References:

Internet Security Systems X-Force Database, Multiple vendor Web servers HTTP TRACE method information disclosure, http://xforce.iss.net/xforce/xfdb/11149
Internet RFC/STD/FYI/BCP Archives, Hypertext Transfer Protocol -- HTTP/1.1, http://www.faqs.org/rfcs/rfc2616.html

M **IisImproperHttptrackLogging: Microsoft Internet Information Server (IIS) fails to properly log HTTP TRACK requests**

Additional Information *More Information*

port=80

Microsoft Internet Information Server (IIS) versions 4.0 and 5.0 could allow a remote attacker to obtain sensitive information. Microsoft Internet Information Server (IIS) fails to properly log HTTP TRACK requests. By sending a specialy-crafted HTTP TRACK request, a remote attacker could cause the server to disclose sensitive information without the request being logged.

Remedy:

Upgrade to the latest version of Microsoft IIS (6.0 or later), available from the Microsoft Web site. See References.

References:

AQTRONIX Security Advisory AQ-2003-02, Microsoft IIS Logging Failure,
http://www.aqtronix.com/Advisories/AQ-2003-02.txt
CERT Vulnerability Note VU#288308, Microsoft Internet Information Server (IIS) vulnerable to cross-site scripting via HTTP TRACK method, http://www.kb.cert.org/vuls/id/288308

M **IisWebdavRunning: Microsoft IIS WebDAV service is running on the system**

Additional Information *More Information*

port=80

Web Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web. WebDAV has been detected as running. Some versions of WebDAV have serious vulnerabilities.

Remedy:

Verify that Microsoft webdav Service is running on the system for legitimate reasons. If use of webdav is required, ensure that security settings had been configured or patches had been applied for best security practices. If use of webdav is not required or if it was enabled under suspicious circumstances, disable it from the system.

IIS administrators may temporarily disable WebDAV support on IIS 5 servers if possible. Microsoft Knowledge Base Article 241520 describes the process in detail. See References.

References:

Microsoft Knowledge Base Article 241520, How to Disable WebDAV for IIS 5.0,
http://support.microsoft.com/default.aspx?scid=kb;[LN];241520
Internet Security Systems X-Force Database, Microsoft IIS WebDAV long request buffer overflow,
http://xforce.iss.net/xforce/xfdb/11533
Internet Security Systems Security Alert, March 17, 2003, Microsoft IIS WebDAV Remote Compromise Vulnerability,
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=22029

L **Iis404SpCheck: Microsoft Internet Information Server 404 error message determines service pack level**

Additional Information *More Information*

port=80

Microsoft Internet Information Server (IIS) varies the length of its Not Found (404) error message depending on the service pack level that has been applied. Remote servers running service packs that are lower than the current IIS service pack may be vulnerable. Attackers can use this information to better focus a structured attack on the server or its computing resources.

Remedy:

Apply the appropriate patch to your system, if the service pack running on the server is lower than the current service pack available. See References.

Consider creating a custom error page that does not display the current service pack level.

References:

Microsoft Web site, Microsoft TechNet - Microsoft Internet Explorer,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=16&servicepackid=0&submit1=go&isie=yes

L **IisAuthenticationErrorMessages: IIS authentication error messages reveal configuration information (CAN-2002-0419)**

Additional Information *More Information*

port=80

Microsoft Internet Information Server (IIS) supports anonymous access, Basic, and NTLM authentication. The authentication mechanism in IIS versions 4.0, 5.0, and 5.1 could reveal the type of authentication being used to a remote attacker. A remote attacker can send a specially-crafted GET request to verify the authentication type being used, depending on the error message returned.

Remedy:

No remedy available as of March 2002.

As a workaround, refer to the recommendations as listed in NGSSoftware Insight Security Research Advisory #NISR04032002. See References.

References:

NGSSoftware Insight Security Research Advisory #NISR04032002, Considerations for IIS Authentication,
http://www.nextgenss.com/advisories/iisauth.txt

L **IisRunning: Microsoft IIS is running on the system (CAN-1999-0633)**

Additional Information *More Information*

IIS_version=5.0

Microsoft Internet Information Server (IIS) is running on this computer. IIS is a Web server platform that is included in some common installations of Microsoft Windows NT and Windows 2000. IIS includes many important features, but for best security practices, it should only be present if Web services are needed on the system. When running IIS, it is important to ensure that the proper security settings are configured for best security practices.

Remedy:

If this system is designed to host Web content, then verify that the installation of IIS has been configured according to your corporate security policy, or use the IIS security checklist provided by Microsoft. See References. If Web services are not needed on this system, then disable IIS.

References:

Microsoft TechNet, Microsoft Internet Information Server 4.0 Security Checklist,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iischk.asp
Microsoft TechNet, Secure Internet Information Services 5 Checklist,
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iis5chk.asp