

Scan Results

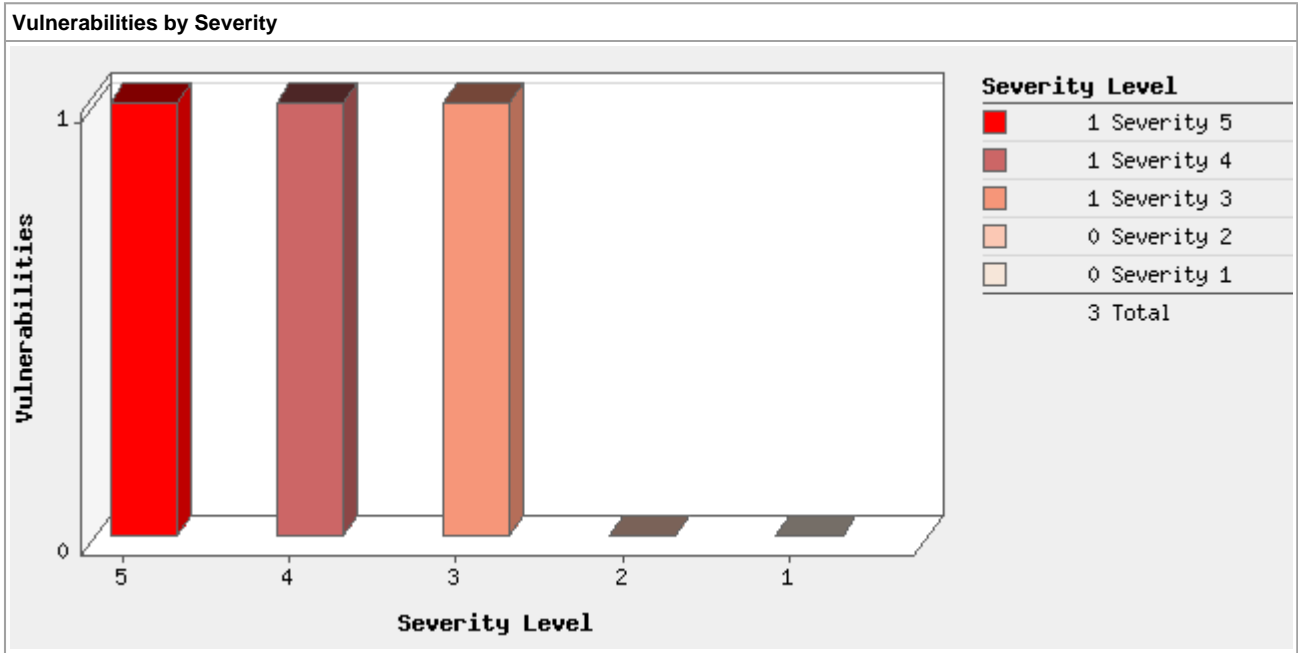
This report was generated with an evaluation version of QualysGuard

05/02/2005

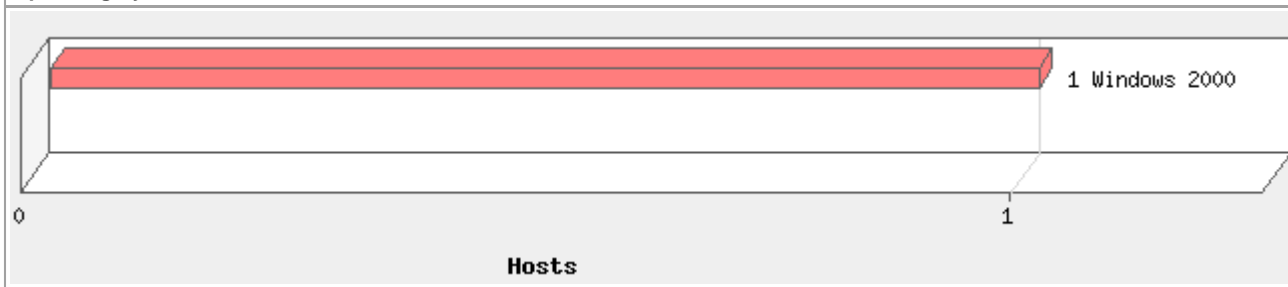
Report Summary	
Company:	Fujitsu
User:	富士通 ITマネージセンター (Manager)
Template Title:	Scan Results
Active Hosts:	1
Total Hosts:	1
Scan Type:	On demand
Scan Status:	Finished
Scan Title:	Sample report
Asset Groups:	Sample report
Target:	127.0.0.1
Options:	Sample report
Filters:	Vulnerability Checks: Disabled checks, Ignored checks
Scan Date:	05/02/2005 at 10:09:46
Reference:	scan/1114996199.4616
Scanner Appliance:	62.210.136.134 (Scanner 2.9.44-1, Web 4.0.139-1, Vulnsigs 1.11.6-4)
Duration:	00:03:26
Default Option Profile:	No

Summary of Vulnerabilities

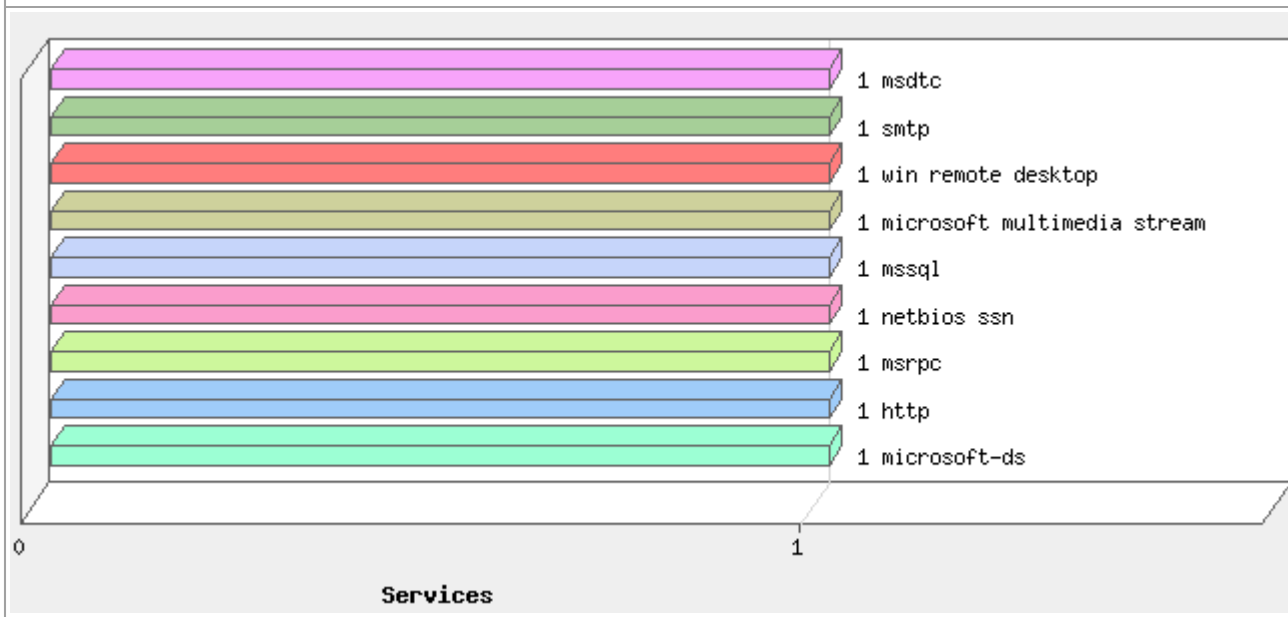
Vulnerabilities Total	10	Average Security Risk	 5.0
-----------------------	----	-----------------------	---



Operating Systems Detected



Services Detected



Detailed Results

127.0.0.1 (sample_report.example.com)

Windows 2000

Vulnerabilities Total	10	Security Risk	5.0
-----------------------	----	---------------	-----

▼ Vulnerabilities (3)

- ▼ 5 Microsoft Index Server および Indexing Service に ISAPI 拡張子のバッファオーバーフローの脆弱性 (Microsoft Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability) sample_report.example.com:80/tcp

QID: 86170 **Category:** Web server **CVE ID:** [CVE-2001-0500](#)

Vendor Reference: MS01-033

THREAT:

Microsoft Index Server および Indexing Service は Web ブラウザ経由のインターネット、もしくはイントラネットサイト上でのテキスト検索を可能にします。Index Server は Windows NT 4.0 Option Packに、Indexing Service は Windows 2000 にそれぞれ同梱しています。

未確認のバッファが Index Server および Indexing Service に関連する ISAPI 拡張子に存在します。Microsoft Index Server または Indexing Service を実行中のホストは ISAPI 拡張子“idq.dll”に未チェックのバッファがあることから、任意のプログラムを実行されやすくなります。“idq.dll”がインストールされたホストに特別な手法でリクエストが送信された場合、Index Server あるいは Indexing Service はバッファオーバーフローを起こし、任意のプログラム実行を許可します。残念ながら、Index Server および Indexing Service は Local System コンテキストで動作します。そのため、攻撃者が Local System 権限で特定の任意のプログラムを実行することが可能です。

“idq.dll”は Internet Data Administration (.ida) ファイルと Internet Data Query (.idq) ファイルのサポートを備えています。“idq.dll”で“.idq”および“.ida”ファイルに関連するスクリプトマッピングが存在しなければ、この脆弱性を利用することはできません。

Index Server や Indexing Service が動作してなくても、攻撃者はこの問題を利用できることにご注意ください。IIS がインストールされる際に“idq.dll”はデフォルトでインストールされます。つまり、IIS さえ動作していれば、脆弱性を利用することができます。

IMPACT:

この脆弱性の利用に成功した場合、ターゲットホストを危険な状態にすることになります。

SOLUTION:


Microsoft は、以下のパッチをリリースしてこの問題を解決しました：

- [Windows NT 4.0 用のパッチ](#)
- [Windows 2000 用のパッチ](#)

RESULT:

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 02 May 2005 01:09:25 GMT
Connection: close
Content-Type: text/html

<HTML>The IDQ file NULL.ida could not be found.

▼  4 Microsoft IIS の管理用ページにおけるクロスサイトスクリプティング脆弱性 (Microsoft IIS Administrative Pages Cross-Site Scripting Vulnerability) sample_report.example.com:80/tcp

QID: 10977 **Category:** CGI **CVE ID:** [CAN-2002-1181](#) [CAN-2002-0869](#) [CAN-2002-1180](#) [CAN-2002-1182](#)
Vendor Reference: MS02-062

THREAT:

Microsoft IIS は、クロスサイトスクリプティング攻撃に対して脆弱です。この脆弱性は、IIS がユーザの提供する入力のある有害部分を適切に無害化しないことが原因です。管理目的で IIS が提供する数多くの Web ページは、ユーザが行う入力をきちんと無害化しません。URI に含まれている可能性のある、悪意のある HTML コードが実行される可能性があります。

IMPACT:

この脆弱性は、脆弱なソフトウェアが動作している Web サイトの正当なユーザから、cookie ベースの認証資格を盗むために利用される可能性があります。この情報をもとに、攻撃者は cookie ベースの認証資格を使用して、正規のセッションをハイジャックする可能性があります。

SOLUTION:

Microsoft は、この問題に対してパッチを提供しています。 [Microsoft Security Bulletin MS02-062](#) を参照してください。


また、このパッチは以下の問題も修正します。これらの問題は、ホストが恐らく脆弱であると思われる問題です：

CAN-2002-0869: アウトプロセスの特権昇格
CAN-2002-1182: WebDAV におけるサービス不能 (DoS)
CAN-2002-1180: スクリプトソースへのアクセス脆弱性

セキュリティ上 IISHelp ディレクトリへのアクセスを常に制限するのが賢明です。

RESULT:

GET
/iishelp/iis/htm/asp/iiatmd1.asp?ScriptLanguagePreference=<script>alert(4098)</script>
HTTP/1.1
Host: sample_report.example.com
Connection: Keep-Alive

▼  3 Microsoft IIS の HTTP リクエストに関するクロスサイトスクリプトの脆弱性 (Microsoft IIS HTTP Redirect Cross Site Scripting Vulnerability) sample_report.example.com:80/tcp

QID: 10564 **Category:** CGI **CVE ID:** [CVE-2002-0075](#)
Vendor Reference: N/A

THREAT:

クロスサイトスクリプト問題は IIS のいくつかのバージョンに存在しています。IIS によって作成された HTTP のリダイレクトページには、ある状況下において不適切なユーザの入力が入っている HTML コンテンツが含まれている可能性があります。

攻撃者はこの脆弱性を利用することにより、脆弱なサーバへのリンクを作成するかもしれません。罪のないユーザがこのリ

リンクをたどると、そのスクリプトコードはそのサーバによって複製されて、脆弱なサイトのコンテキスト内で実行されることとなります。これは、重要なデータとクッキー情報の漏洩をもたらすか、攻撃者にサイトのコンテンツと機能を破壊されてしまいます。

IMPACT:

この脆弱性が利用されることにより、悪意のあるユーザに重要なデータとクッキー情報を取得されるか、サイトの内容と機能を破壊されてしまいます。

SOLUTION:

Microsoft は、この問題に対してパッチを提供しています。Microsoft Security Bulletin MS02-018を参照してください。
[Microsoft Security Bulletin MS02-018](#)

Microsoft IIS Site Server を稼働しているユーザのための累積パッチに関する問題が報告されています。累積パッチをインストールした結果副作用として起こった問題に対処する hotfix は Microsoft によってリリースされています。累積パッチをインストールした結果問題が起こったユーザは Microsoft サポートに連絡し、hotfix Q317815 を要求してください。

RESULT:

```
GET /scripts?><script>alert("no9_such71_dir38");</script> HTTP/1.0
Host: sample_report.example.com
```

HTTP/1.1 302 Object Moved

Location:

```
http://sample_report.example.com/scripts/?><script>alert("no9_such71_dir38");</script>
```

Server: Microsoft-IIS/5.0

Content-Type: text/html


Content-Length: 202

```
<head><title>Document Moved</title></head>
```

```
<body><h1>Object Moved</h1>This document may be found <a
```

```
href="http://sample_report.example.com/scripts/?><script>alert("no9_such71_dir38&quot;
ot;)</script>">here</a></body>
```

▼ Potential Vulnerabilities (3)

- ▼  5 Microsoft IIS 5.0 におけるインプロセステーブルの権限昇格の脆弱性 (Microsoft IIS 5.0 In-Process Table Privilege Elevation Vulnerability) sample_report.example.com:80/tcp

QID: 86196 **Category:** Web server **CVE ID:** [CVE-2001-0507](#)

Vendor Reference: MS01-044

THREAT:

パフォーマンス上の理由により、Microsoft Internet Information Server (IIS) 5.0 は、リモートからリクエストされた際に特定のプログラムを“インプロセス”で動作する機能があります。

プログラムは“インプロセス”で動作する場合、メインの IIS プロセスの一部として動作します。この場合、プログラムはローカルシステムのセキュリティコンテキスト上で実行されるので、どのプログラムが“インプロセス”で動作できるのかを制限することが重要です。

IIS 5.0 は、Web クライアントにリモートからリクエストされた場合に“インプロセス”で動作するようなプログラムテーブルを同梱しています。これらのバイナリは全て IIS に同梱されていますが、相対パスでテーブルに一覧が記載されます。IIS サーバにファイルを作成することができるユーザは、テーブルのエントリと同じ相対パスとファイル名で、Web root ファイルシステム上にプログラムを置くことができます。このプログラムの実行が要求されると、パスとファイル名が一致しているため、プログラムは“インプロセス”で実行されます。このプログラムは、権限のないユーザに対して、管理者用アクセス権を与える可能性があります。

デフォルトでは、権限のないユーザは、IIS サーバへコンテンツをアップロードすることを許可されていません。

IMPACT:

Web ルートへの書き込み権を持っているローカルユーザは、“Local System” (管理者) 権限を獲得する事ができます。

また、リモートユーザが何とか Web サイトへの書き込みアクセスを入手しようとするイベントにおいて、このバグが利用される可能性があります。このようなイベントは起こる可能性は低いです。しかし、そのようなリモートユーザが既に(このバグがないまま) Web サイトコンテンツを変更できるような場合は、サイトの改変が導かれます。あるいは、カスタム CGI スクリプトをサイト上に設置できるのであれば、サーバ上で任意のプログラムが実行されることとなりますので、ご注意ください。


注意事項: ローカルセキュリティホールについて、QualysGuard ではお使いのマシンの脆弱性をテストすることはできません。従って、お客様がお使いのマシンにすでに適切なパッチを適用されている場合は、この警告を安全に無視することができます。

SOLUTION:

Microsoft は、この問題に対してパッチを提供しています。 [Microsoft Security Bulletin MS01-44](#) を参照してください。

RESULT:

No results available

▼  4 Microsoft IIS HTR のチャンクされたエンコード転送のヒープオーバーフローにおける脆弱性(Microsoft IIS HTR Chunked Encoding Transfer Heap Overflow Vulnerability) sample_report.example.com:80/tcp

QID: 10751 **Category:** Web server **CVE ID:** [CVE-2002-0364](#)

Vendor Reference: MS02-028

THREAT:

ISAPI HTR エクステンションに関連する“チャンクされたエンコード転送機構”内のヒープオーバーフロー状態が Microsoft IIS (Internet Information Services) で発見されました。

この状態は HTR を実行する ISAPI エクステンションによって動的に割り当てられる未確認のバッファに原因があります。HTR スクリプティングは、ASP (Active Server Pages) を優先して広範囲で使用されることはありませんでした。この脆弱性は HTR ISAPI フィルタが有効になっているシステム上でのみ問題を生じます。

この脆弱性は、IIS 4.0 と IIS 5.0 に影響を及ぼします。この脆弱性の利用は、サービス不能またはリモートの攻撃者が被害を受けているホスト上で任意の指示を実行させるという結果を導きます。攻撃者は静的グローバル変数の上書き、保存された関数ポインタ、プロセス管理構造、メモリ管理構造、そして攻撃者提供による指示などの悪意のあるセッションを開始することが可能です。

IIS 4.0 において、任意のプログラムの実行で完全に危険な状態になる可能性があります。IIS 5.0 において、この問題は多少ではあるがそれでもなお重要な特権を得ることを攻撃者に許可します。

この脆弱性は Bugtraq ID 4485 および Microsoft Security Bulletin MS02-018 で述べられている問題と似ています。違いはこの問題は HTR ISAPI エクステンションを限定して影響を及ぼすということです。

IMPACT:


攻撃者は静的グローバル変数の上書き、保存された関数ポインタ、プロセス管理構造、メモリ管理構造、そして攻撃者提供による指示などの悪意のあるセッションを開始することが可能です。

SOLUTION:

Microsoft は、この問題に対してパッチを提供しています。 Microsoft Security Bulletin MS02-028 を参照してください。 [Microsoft Security Bulletin MS02-028](#)

RESULT:

No results available

▼  3 Microsoft IIS 4.0/5.0 不正なファイル拡張子による DoS の脆弱性 (Microsoft IIS 4.0/5.0 Malformed File Extension DoS Vulnerability) sample_report.example.com:80/tcp

QID: 86158 **Category:** Web server **CVE ID:** [CVE-2000-0408](#)

Vendor Reference: N/A

THREAT:

Microsoft IIS 4.0 および 5.0 にはサービス不能 (DoS) の脆弱性が含まれています。適切なパッチを既に適用している場合は、この警告を安心して無視されても構いません。

不正なファイル拡張し情報を含む、特別に作成された URL を Microsoft IIS 4.0 または 5.0 へ送ることにより、悪意のあるユーザはすべての CPU を消費することができ、プログラムのサービスを停止させます。

IMPACT:

結果として、通常の機能を回復するためにはアプリケーションを再起動するか URL が処理されるのを待つ必要があります。


SOLUTION:

Microsoft はこの問題を修正するパッチをリリースしています。 [Patch Q260205](#) (英語)

RESULT:

No results available

▼ **Information Gathered (4)**

▼  2 OS の検出 (Operating System Detected)

QID: 45017 **Category:** Information gathering **CVE ID:** N/A
Vendor Reference: N/A

THREAT:

ホスト上の操作システム (OS) を特定するために、さまざまな異なる技術を使用することができます。これらの技術の簡単な説明を以下に提供しています。このホスト上で OS を特定するために使用した、具体的な技術はレポートの RESULTS セクションに含まれています。

1) **TCP/IP のフィンガープリント:** ホストの OS を、TCP/IP のフィンガープリントを使用してリモートシステムから特定することができます。すべての下層 OS の TCP/IP スタックには微妙な違いがあり、特別に作成した TCP パケットに対する返信でその違いがわかります。この“フィンガープリント”技術の結果によると、OS バージョンは以下の一覧のうち、いずれかです。

スキャナとホストの間にあるファイアウォールやパケットフィルタリングデバイスによって、これらの微妙な違いが 1 つ以上修正されている場合、フィンガープリントの技術は失敗する可能性があることにご注意ください。その結果、OS のバージョンが正確に検出されない可能性があります。ホストが proxy 型のファイアウォールの背後にある場合、検出された OS のバージョンは、スキャンされたホストではなくファイアウォールのバージョンである可能性があります。

2) **NetBIOS:** Network Basic Input Output System の省略形が NetBIOS です。NetBIOS は、ローカルエリアネットワーク (LAN) 用の特別な機能を追加して DOS BIOS を補強した、アプリケーションプログラミングインタフェース (API) です。ほぼすべての PC 用 LAN は、NetBIOS がベースになっています。LAN メーカーの中には、追加のネットワーク能力を付け足して、機能を拡張しているメーカーすらあります。NetBIOS は Server Message Block (SMB) というメッセージフォーマットに依存しています。

3) **PHP Info:** PHP は、ハイパーテキストプリプロセッサです。動的 Web ページを作成するために使用される、オープンソースでサーバサイドの、HTML 埋め込み型スクリプト言語です。ある設定では、phpinfo() のような PHP 関数を呼び出し、OS の情報を得ることができます。

4) **SNMP:** Simple Network Monitoring Protocol を使用して、ホストやルータ、そしてそれに付随するネットワークを監視することができます。SNMP サービスは、Management Information Base (MIB) という、管理者が取り出すことができる一連の変数 (データベース) を保持しています。これらには、OS 用の “MIB-II.system.sysDescr” 変数が含まれています。

IMPACT:


N/A

SOLUTION:

N/A

RESULT:

Operating System	Technique	ID
Windows 2000	TCP/IP Fingerprint	U1263
Windows 2000 Server	SRVSVC	Interface
Windows 5.0/Windows 2000 LAN Manager	CIFS via TCP Port 445	

▼  1 ICMP からの返信を受信 (ICMP Replies Received)

QID: 82040 **Category:** TCP/IP **CVE ID:** N/A
Vendor Reference: N/A

THREAT:

ICMP (Internet Control and Error Message Protocol) は、IP パケットにカプセル化されたプロトコルです。ICMP の主要な目的は、ゲートウェイの内部接続性および他のゲートウェイまたはホストのアクセス能力を伝えるプロトコル層を提供することです。

ホストが ICMP 返信を送信するよう、以下の型のパケットを送信しました:

- Echo Request (Echo Reply を誘発するため)
- Timestamp Request (Timestamp Reply を誘発するため)
- Address Mask Request (Address Mask Reply を誘発するため)
- UDP Packet (Port Unreachable Reply を誘発するため)
- IP Packet with Protocol >= 250 (Protocol Unreachable Reply を誘発するため)

“結果”のセクションに表示されている一覧が、受信した ICMP 返信です。


RESULT:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

Timestamp (type=14 code=0)
Unreachable (type=3 code=2)
Unreachable (type=3 code=3)

Timestamp Request
IP with High Protocol
UDP

07:21:30 GMT
Protocol Unreachable
Port Unreachable

▼  1 公開されている TCP サービスのリスト (Open TCP Services List)

QID: 82023 **Category:** TCP/IP **CVE ID:** N/A
Vendor Reference: N/A

THREAT:

ポート・スキャナは、権限のないユーザがツールを利用して、インターネットからアクセスできるこのホスト上の全てのサービス情報を取得することを可能にします。このテストは"ステルス"ポート・スキャナで実行したため、サーバには実際の接続ログは記録されません。

IMPACT:

ポートスキャナで取得した情報を利用し、権限のないユーザが、公開されているサービスの脆弱性をテストすることが可能です。

SOLUTION:

リスト上の不明な、あるいは未使用のサービスをシャット・ダウンしてください。もしどのサービスがどのプロセスやプログラムによって提供されているか不明な場合は、Qualys緊急対応チームに連絡するか、または、この種のポート・スキャナの検知に利用される商用あるいはオープン・ソースの侵入検知システムについて、より詳細な情報を提供しているCERTのwebサイトをご覧ください。

RESULT:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
25	smtp	Simple Mail Transfer	smtp	
80	www	World Wide Web HTTP	http	
135	msrpc-epmap	epmap DCE endpoint resolution	msrpc	
139	netbios-ssn	NETBIOS Session Service	netbios ssn	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
1433	ms-sql-s	Microsoft-SQL-Server	mssql	
1755	netshow	ms-streaming	Microsoft Multimedia Stream	
3372	tip2	TIP 2 / MSDTC	msdtc	
3389	ms-wbt-server	MS WBT Server	win remote desktop	
6666	ircu	IRCU	unknown	

▼  1 Web サーバのバージョン (Web Server Version) sample_report.example.com:80/tcp

QID: 86000 **Category:** Web server **CVE ID:** N/A
Vendor Reference: N/A

RESULT:

Server Version	Server Banner
Microsoft-IIS/5.0	Microsoft-IIS/5.0

This report was generated with an evaluation version of QualysGuard

CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free.