

# What Are the Most Dangerous Internet Services?

Of the wide array of Internet services that provide e-mail, authentication, interactive access, web pages, chat rooms, etc., have you ever wondered which services are the most vulnerable and dangerous to your company?

We could debate for several weeks what criteria to use to make such a judgment but without holding a conference in Hawaii to take the first step, Cisco Secure Consulting Services has made some assumptions and posted the answers: *e-mail* and *web* services are the most dangerous. Why? Because if you graph the most common services found on the Internet against how often these services were found to have security holes, e-mail and web services rank at the top. Practically every company who has an Internet presence offers these services. They affect virtually every Internet user and the security of corporations.

If you only wanted the answer, you can stop now. If you want to know more about how to answer other questions (such as “Before opening up that hole in your router’s ACL or firewall to support yet another application, how do you quantify the risk to your company?”), keep reading and visit the Cisco Secure Encyclopedia (CSEC) at [www.cisco.com/go/csec](http://www.cisco.com/go/csec).

CSEC has real statistics that were taken from live data networks during actual security assessments. These results are not based on guesses or questionnaires but on raw numbers taken from real corporate environments.

## The Full Story

The Cisco Secure Consulting Services group regularly tests corporate networks for security flaws. Uncovering security holes in operating systems, network devices, authentication schemes, and security architectures is a typical day for the Cisco Network Security Engineers. If you asked security consultants to identify the most vulnerable and dangerous services on the Internet, each would have a very different story. But what if you had access to a data warehouse that contained over four years of security data on corporate America? Intriguing?

While working on this project, I found myself debating the meaning of “the service that is the most vulnerable” (for example, was it the most misconfigured, did it have programming flaws, etc.) because we might have seen it only once out of 1000 IP addresses. My conclusion was to cross how often we found an Internet service with how often we found that service with a security problem. This graph yielded me a measure of the most dangerous Internet service:

Most Common + Most Vulnerable = Most Dangerous

Does this mean that your corporate network is at risk if you provide this service? Yes.  
Does this mean that your corporate network can be exploited? Not definitively.

Any network connected to the Internet is at risk. The job of your corporate security manager is to assess the risk and mitigate it according to the cost. It is valuable to know what history has shown to be a high-risk service and to review the counter measures that you have in place to prevent abuse of the service. The question must be, what is *your* most dangerous Internet service?

When the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon ([www.cert.org](http://www.cert.org)) publishes a new security advisory, it can be difficult to understand if it is a real issue and if it affects you. How do you know if this vulnerability has been seen (or ever will be seen) outside of a test lab? For example, imagine that a new network service vulnerability within an RPC (Remote Procedure Call) family of programs has just been publicly disclosed. Maybe it is in ToolTalk, *cmsd*, or *sadmin*. Although CSEC might not have much historical data on the new buffer overflow in *snmpxdmid*, it can easily tell you that when RPC programs are available to the Internet, overall 93.4 percent have reported some vulnerability. A further breakdown might show that in your business sector, 85.1 percent have been found to be vulnerable. Obviously, any RPC security issue should be at the front of your watch list (if for no other reason than because RPC security flaws typically yield the attacker remote *root* access to your system).

### **Most Common Internet Services**

Ranked by sheer volume, Table A shows the most common services that have been visible to the Internet. Your company should have a clear understanding of what is exposed to the Internet and the risk associated with those services. The most common network service found on the Internet is SNMP (Simple Network Management Protocol). It is not really surprising that this protocol for managing and monitoring network devices made it to the top of the list, but what is surprising is that it is not always seen as a large security risk. There is no need to allow the Internet at large to make SNMP requests to your devices. What you might give up is full control of the device.

The second most frequently seen service is Telnet. The risks of running Telnet and other forms of authentication should be obvious. Any time you allow customers or staff members to authenticate via the Internet, using proper passcodes, one-time passwords, or tiered authentication is a must.

Probably the most obvious choice for Table A is ranked third: HTTP or web services. These services provide the Internet with search engines, home pages, and interactive information via web browsers.

Table A. Most Common Internet Services

Ranking / Service / % Found	
1. SNMP	12.2
2. Telnet	10.5
3. HTTP	9.8
4. FTP	7.1
5. SMTP	6.6
6. finger	4.8
7. DNS	4.6
8. rsh	3.9
9. RPC	3.8
10. TFTP	3.4

### Most Vulnerable Internet Services

The most vulnerable Internet services are ranked by the percentage of times that the service was visible and found to have a security problem. According to Table B, RPC is clearly the winner (or is that the loser)? Of the times that RPC, (a.k.a. the *portmapper*) has been found to be active, 93.4 percent of the systems had one or more reported security problems. Although every vulnerability within a service has its own level of severity, security problems with RPC are generally ranked as having a high severity. Because the *portmapper* executes programs as a privileged user, unpatched problems with RPC give remote attackers complete control over the system.

Taking second place in the most vulnerable service table is SMTP. If an SMTP or e-mail server is accepting Internet connections, there is a 61.1 percent chance that it will have a misconfiguration or be running outdated software that contains security bugs. Bugs and misconfigurations might vary in severity from giving out username information (usually one-half of the authentication equation) to allowing an attacker to start a privileged program.

Table B. Most *Vulnerable* Internet Services

Ranking / Service / % Vulnerable	
1. RPC	93.4
2. SMTP	61.1
3. finger	59.6
4. TFTP	57.4
5. HTTP	42.4
6. DNS	35.0
7. FTP	33.0
8. NFS	30.2
9. SNMP	27.1
10. X Window System	23.0

## Most Dangerous Internet Services

Combining Tables A and B provided more insight into the significance of a vulnerability. Only seven services were common between both tables. After graphing the seven on an X,Y scatter chart (Chart A), I eliminated services that fell into the lower left quarter: the deleted services were neither the most common nor the most vulnerable.

With FTP, DNS, and *finger* falling out of consideration, two groups formed. Group 1 consisted of SNMP and RPC, services that should not have been accessible to the Internet at large and that fall on the extreme corners of the chart. Group 2 contains HTTP and SMTP, which are critical Internet business components.



There is little, if any, justification for accepting RPC and SNMP requests from the Internet at large. Because RPC brokers requests for dozens of other programs, it can be difficult to manage and secure. Strongly consider disabling the *portmapper* or blocking TCP port 111 at your edge device. If SNMP is a necessity, allow queries only from a small list of trusted IP addresses.

Most companies, however, have valid business needs for accepting web traffic and e-mail from anywhere in the world. Dropping these services is not an option. Most vulnerabilities found in web services relate directly to the web server vendor or to the vendor of add-on software, and are far too numerous to be covered here. For example, recent vulnerabilities in Microsoft's IIS web server allow an attacker to view any file in the web root and remotely execute arbitrary code. In most cases, this allows the attacker to take full control

of the server. Running an up-to-date vulnerability scanning tool against your web server is one of the most effective methods to provide piece of mind. A list of the security holes for web services that can be exploited from the Internet can be found in CSEC by searching for “HTTP.”

Several of the most vulnerable services do not appear in Chart A. This means that while the services were quite vulnerable, they are not normally running on Internet-accessible systems. NFS (Network File System) is a good example. When NFS was seen via the Internet, it was vulnerable 30.2 percent of the time. However, most companies realize the futility and risk in using NFS over the Internet and are not doing it. Another example that diminishes the security significance of a single vulnerabilities list is the X Window System, which was found vulnerable 23.0 percent of the time but is seldom seen from the Internet. These show the importance of understanding the context of any statistics that you read.

## **Conclusion**

There are numerous areas in Internet security that are not represented in our data, such as e-mail viruses, Trojan code attachments, mobile code, individual web browser settings, or misuses of e-mail to leak corporate secrets. Our data addresses primarily network services and external exposures. Because the consulting service gathers new data daily, specific percentages will also change. However, for almost every company, the following advice applies:

- Consolidate your Internet presence to reduce your company’s “Internet footprint.” Provide to the Internet only those services that are necessary to market your business and provide services to your customers. Reducing allowable services decreases risk and maintenance.
- Determine a baseline measurement of your network traffic. Know what is normal for your network and what is not.
- Implement an e-mail gateway or proxy to filter and check e-mail for proper business policies. Issues include checking for viruses, size, suspect addresses, and inappropriate content.
- Regularly scan your Internet-visible devices for services and for specific service vulnerabilities.

Cisco customers, business partners, and the Internet community can access our assessment data to help clarify and add reality to confusing cybersecurity issues.

[www.cisco.com](http://www.cisco.com)

[www.cisco.com/go/csec](http://www.cisco.com/go/csec)

[www.cisco.com/go/securityconsulting](http://www.cisco.com/go/securityconsulting)