RAPID7

USA
RANK 1
OF 187

NATIONAL EXPOSURE INDEX

THE UNITED STATES | 2018

In 2016, Rapid7 Labs launched the National Exposure Index in order to get a measurable, quantitative answer to a fairly fundamental question: What is the nature of internet exposure—services that either do not offer modern cryptographic protection, or are otherwise unsuitable to offer on the increasingly hostile internet—and where, physically, are these exposed services located?

Now in our third year, we continue this ongoing investigation into the risk of passive eavesdropping and active attack on the internet, and offer insight into the continuing changes involving these exposed services. We've also added a third dimension for exposure, "amplification potential," where inappropriately exposed UDP services can be used in amplified, distributed denial of service (DDoS-A) attacks.

Overall Key Findings

- The United States ranks as the most exposed in the 2018 National Exposure Index, scoring the highest in nearly every exposure metric we measure. Following the U.S. is China, Canada, South Korea, and the United Kingdom, which together control over 61 million servers listening on at least one of the surveyed ports.

- There are 13 million exposed endpoints associated with direct database access, half of which are associated with MySQL. Along with millions of exposed PostgreSQL, Oracle DB, Microsoft SQL Server, Redis, DB2, and MongoDB endpoints, this exposure presents significant risk of crucial data loss in a coordinated attack.

- While the number of exposed Microsoft SMB Servers dropped considerably after the WannaCry attack of 2017, there remain about a half a million targets today, primarily in the U.S., Taiwan, Japan, Russia, and Germany.

- Amplification-based distributed denial of service (DDoS-A) remains a powerful technique for harming enterprises and providing cover for more sophisticated attacks. While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.

These key findings tell us that the most risk to the internet originates in countries that have significant investment in, and reliance on, a safe and stable internet. This indicates to us that national internet service providers in these countries can use these findings to understand the risks of internet exposure, and that they, along with policymakers and other technical leaders, are in an excellent position to make significant progress in securing the global internet.

Key Statistics for The United States

Country (ISO3C)	The United States (USA)
Rank	1
IPv4 Allocated Address Space	1,605,538,816
Responsive IPv4 Servers (Percentage)[1]	42,039,250 (2.62%)
Encrypted Web Ratio[2]	44.22%
Encrypted Shell Ratio[3]	89.58%
Exposed SMB Total (Percentage)[4]	1,158,041 (2.75%)
Exposed Database Total (Percentage)[5]	6,146,982 (14.62%)
Inappropriate UDP Total (Percentage)[6]	900,576 (2.14%)

Key Findings for The United States

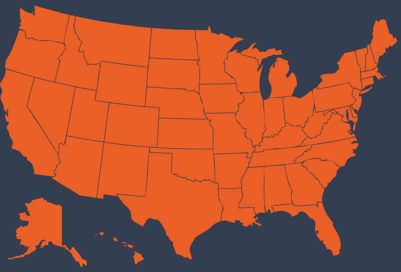
The United States tops the rankings for the 2018 National Exposure Index, coming in **1st** in the overall most exposed nations on Earth. Given that our new ranking accounts for overall, absolute numbers of exposed servers and services, this comports to our intuition—after all, the United States has a massive allocation of IPv4s. There are only 15 countries of the 187 surveyed that have more allocated IPv4 address space than the **42 million active, responsive servers in the United States**, so the target space for attackers is correspondingly huge. If you're in the business of compromising, eavesdropping on, or otherwise abusing internet-exposed servers, the United States is the place to concentrate on.

Of special concern is the outsized population of exposed database servers in the US: 14.62% of all servers are responsive to probes to the most popular database-associated TCP/IP ports, with responses to over **2.5 million MySQL probes** (on port 3306/TCP) and over **1 million Oracle Database probes** (on 1521/TCP). It is never a good idea to directly expose database servers to the internet; rarely are the passwords chosen for such servers sufficiently complex, and database servers do not come with built-in rate-limiting measures to prevent online bruteforcing of those passwords. Database servers are among the most complex software packages ever written, and new vulnerabilities are routinely discovered in them. Often, these vulnerabilities go under-reported, since database servers "shouldn't be exposed to the internet," but we can see that this is not the case in the United States (among other countries).

For Rapid7's complete National Exposure Index, which includes many additional findings related to both national and global exposure metrics, please visit www.rapid7.com/national-exposure.

USA
RANK 1
OF 187

The United States has an allocation of over 1.6 billion IPv4 addresses, and about 42 million servers were responsive to scanning by Rapid7 researchers.



Exposure Index Key

Least Exposed

Most Exposed

[1] The sum of all IPv4 nodes which respond affirmatively to a TCP SYN or a UDP request, over that country's allocated IPv4 space.

[2] The fraction of common HTTPS ports (443 and 8443) over all HTTP and HTTPS ports (443, 8443, 80, 81, 8000, 8080, and 8888)

[3] The fraction of responsive SSH probes on port 22 over the sum of all the SSH and telnet (port 23) responders in that country

[4] The fraction of responsive SMB probes over the total IPv4 utilization figure for that country

[5] The fraction of responsive probes on ports 1433, 1521, 3306, 5432, 6379, 27017, and 50000 over the total IPv4 utilization figure

[6] The fraction of responsive probes on UDP ports 19, 137, 389, 1900, 5353, 5060, and 11211 over the total IPv4 utilization figure