RAPID7

DEU
RANK 9
OF 187

NATIONAL EXPOSURE INDEX

GERMANY | 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 While the number of exposed UDP-based memcached servers is less than 4,000, there are about 40,000 unpatched, out-of-date memcached servers, which are at risk of being drafted into the next record-breaking DDoS attack.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 Germany

Country (ISO3C)	Germany (DEU)
Rank	9
IPv4 Allocated Address Space	120,768,552
Responsive IPv4 Servers (Percentage)[1]	13,430,530 (11.12%)
Encrypted Web Ratio[2]	51.17%
Encrypted Shell Ratio[3]	93.18%
Exposed SMB Total (Percentage)[4]	87,282 (0.65%)
Exposed Database Total (Percentage)[5]	380,722 (2.83%)
Inappropriate UDP Total (Percentage)[6]	6,004,973 (44.71%)

Key Findings for Germany

Germany, from a National Exposure perspective, is doing a lot of things right: It has an incredibly healthy encrypted shell ratio, with over 90% of internet-exposed shell access restricted to SSH, rather than old and cleartext telnet. It also hosts a relatively high ratio of HTTPS, rather than HTTP-based, websites; anything over 35% tends to signal some strong headway toward making HTTPS a default web browsing protocol for a given region, and Germany's crossed the fifty percent line there. Finally, German Windows SMB seems to be all but off the internet — less than 1% of internet facing servers respond affirmatively to probes on SMB's standard port, 445/TCP.

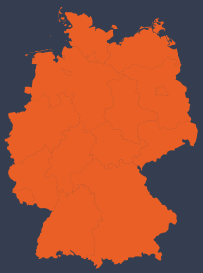
That said, Germany comes in **9th place** among the 187 countries surveyed for one big reason: It has a completely verrückt amount of exposed inappropriate UDP services. During the survey period, Rapid7 counted **over six million exposed UDP services** (excluding NTP and DNS), almost all of which (5.9 million) are the Voice over IP (VoIP) routing protocol, Session Initiation Protocol (SIP) on port 5060/UDP. The closest second place in the top ten most exposed countries is Japan, with 1.87 million SIP servers.

SIP presents a unique exposure for Germany — it is a notoriously difficult protocol to adequately secure against both active and passive eavesdropping for contact lists, traffic analysis, and often some forms of toll fraud and voice communications eavesdropping. Encrypted SIP (SIP-TLS on port 5061/TCP) is really the only way to defend against this, but legacy, cleartext SIP is still immensely popular in Germany.

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.

DEU
RANK 9
OF 187

Germany has an allocation of over 120 million IPv4 addresses, and about 13 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