RAPID7

NICER 2020:
Nordics Edition

THE NORDICS

Rapid7's National / Industry / Cloud Exposure Report (NICER) for 2020 is the most comprehensive census of the modern internet. In a time of global pandemic and recession, the Rapid7 research team offers NICER as a data-backed analysis of the changing internet risk landscape, measuring the prevalence and geographic distribution of commonly known exposures in the interconnected technologies that shape our world. This paper is focused specifically on the unique exposures for the Nordics and dives into the notable highlights and recommendations specific to the following countries: Denmark, Faroe Islands, Finland, Greenland, Iceland, Norway, and Sweden.[2]

Key takeaways include:

- Overall exposure is relatively low (the highest-ranked country, Sweden, is down at No. 26), mostly due to smaller IPv4 allocations and lower numbers of published services.
- Notable exceptions to this low exposure include a large amount of cleartext file transfer protocol (FTP) servers (243,890), along with substantial SSH (163,290), Telnet (19,580), and Remote Desktop Protocol (RDP) (31,017) service counts.
- High vulnerabilities (CVSS 8.5+) are concentrated in a small number of very outdated versions of Samba (Linux/open source version of Microsoft SMB/CIFS file-sharing services), DNS servers, and web/FTP servers, whereas medium-severity weaknesses (CVSS 4-8.4) are in abundance and concentrated in a diverse version distribution of Apache HTTPD servers.

Summary Statistics for the Nordics by Member Country

COUNTRY	RANK	IPV4 ALLOCATIONS	IPV4S DISCOVERED	PERCENT AGE IN USE
Sweden	26	29,957,480	919,526	3.1%
Norway	45	15,931,920	467,468	2.9%
Denmark	51	12,593,128	317,458	2.5%
Finland	60	13,688,000	242,435	1.8%
Iceland	115	888,576	29,153	3.3%
Greenland	149	35,072	14,648	41.8%
Faroe Islands	211	44,032	7,915	18.0%
Summary for Nordics		**73,138,208**	**1,998,603**	**2.73%**

Discovered Services Across All Nordic Countries

SERVICE GROUP	SERVICE NAME	COUNT
Console Access	SSH (22)	163,290
Console Access	Telnet (23)	19,580
Database	memcached (11211)	84
Database	MS SQL (UDP/1434)	1,354
Database	MySQL (TCP/3306)	6
Database	Redis (6379)	241
File Sharing	FTP (21)	243,890
File Sharing	FTPS (990)	2,607
File Sharing	rsync (873)	3,222
File Sharing	SMB (445)	6,442
Infrastructure	DNS (TCP/53)	74,957
Infrastructure	DNS (UDP/53)	85,713

[1] https://rapid7.com/nicer
[2] While Åland Islands and Svalbard and Jan Mayen are perfectly real and, might I say, lovely countries that you should definitely visit someday, their IP space is too small to reliably geolocate or make any statistically significant conclusions about. So, while they should absolutely get your attention in other ways, they will not be covered in this view of Nordic internet exposure.

SERVICE GROUP	SERVICE NAME	COUNT
Infrastructure	DoT (853)	49
Infrastructure	NTP (123)	35,046
Mail	IMAP (143)	36,099
Mail	IMAPS (993)	36,756
Mail	POP3 (110)	33,977
Mail	POP3S (995)	30,761
Mail	SMTP (25)	54,256
Mail	SMTP (587)	35,301
Mail	SMTPS (465)	28,601
Remote Access	Citrix ADC/NetScaler (various)	3,699
Remote Access	RDP (3389)	31,017
Remote Access	VNC (5900+5901)	8,104
Web Primary	HTTP (80)	499,134
Web Primary	HTTPS (443)	433,832

Vulnerability Prevalence by Severity and Country

COUNTRY	HIGH	MEDIUM	LOW
Finland	5,386	336,228	29,925
Sweden	4,585	776,259	26,834
Denmark	1,527	205,033	9,817
Norway	1,514	259,576	9,781
Iceland	107	28,151	1,408
Faroe Islands	2	560	27
Greenland	0	768	39
Summary for Nordics	**13,121**	**1,606,575**	**77,831**

Nordics Service Exposure

This section is similar to the service exposure analysis in the original NICER report but is focused on the most significant non-web protocols found in the Nordics, specifically: Telnet, SSH, RDP, and FTP. While SMB, MS SQL, and all the rest certainly are present in the Nordics, their exposure rates are markedly lower than the global average.

Nordics Service Exposure Focus: Telnet

It wasn't the first console protocol, but it's the stickiest.

SNAPSHOT

WHAT IT IS:	One of the oldest remote console applications in use today on the internet.
HOW MANY:	19,580 discovered nodes
VULNERABILITIES:	Oddly, there are few remote code execution-style vulnerabilities, but plenty of default credentials and opportunities to eavesdrop on the same.
ADVICE:	Never, ever expose Telnet to the internet.
ALTERNATIVES:	SSH (Secure Shell) is the most straightforward alternative to Telnet, but consider the wisdom of exposing console access to the internet in the first place.

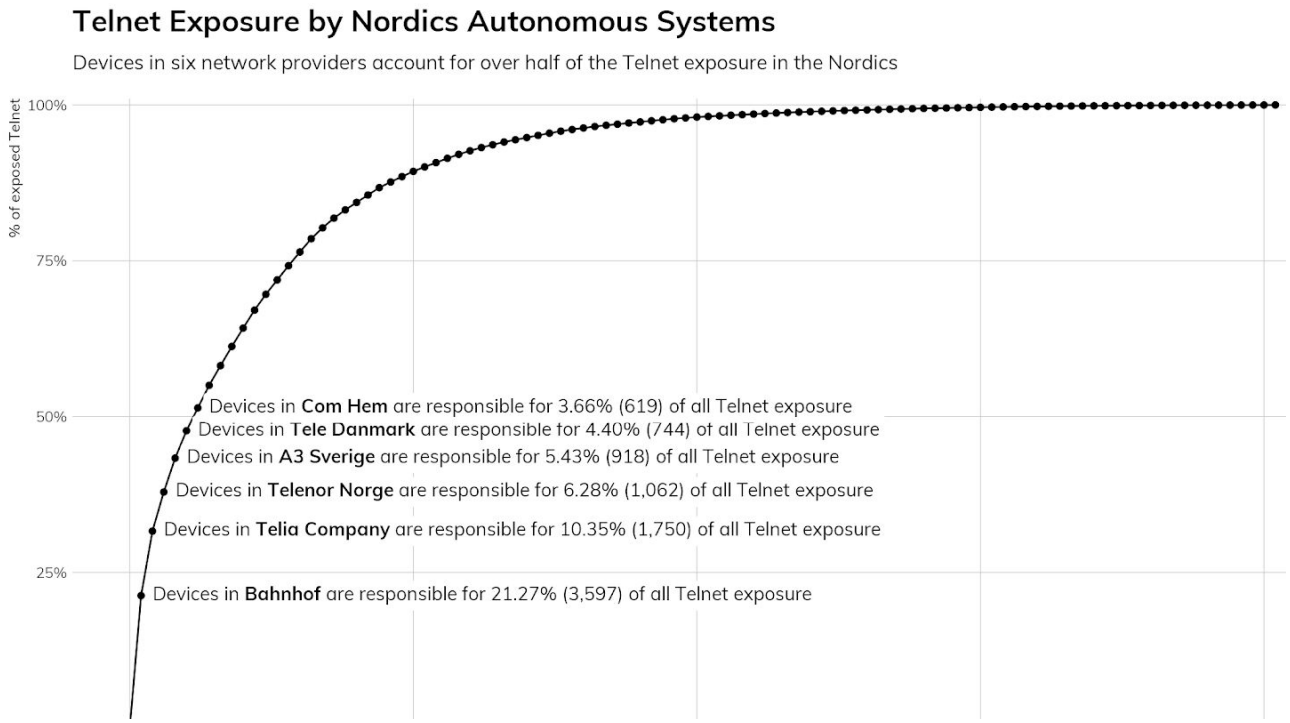
The Nordics View

Telnet can be a difficult service to fingerprint, since the vast majority of login prompts are merely `login:` or `username:`. As such, only 3,610 devices (18%) enabled discovery of device vendor:

VENDOR	COUNT
Cisco	1,150
HP	1,109
Microsoft	620
MikroTik	384
DD-WRT	73
CentOS	52
DrayTek	44
Huawei	37
Juniper	25
Polycom	17
Asus	15
Fortinet	14
Grandstream	11
Hikvision	11
Rifatron	10
Ubuntu	10
SMA Solar Technology Ag	8
Moxa	4
Ricoh	4
NetBSD	2
PowerWare	2
TP-Link	2
ZyXEL	2
FreeBSD	1
IBM	1
SCO	1

Cisco, HP, and MikroTik are all enterprise- or carrier-class routers, meaning network providers or businesses accidentally or deliberately chose to enable Telnet, placing their business-critical traffic at risk. While the presence of "Microsoft" might seem surprising, these are mostly Windows CE-embedded systems, many of which are exposing administrative interfaces to building automation systems.

Over 50% of Nordics Telnet exposure comes from just six network provider autonomous systems.



Devices exposing Telnet in Bahnhof appear to be voice over IP (VoIP) interfaces exposing their Telnet admin port. While most of the Telnet exposure in Telia is somewhat abated by most of the devices refusing to allow a login from non-Telia IP address space, they are still prone to eavesdropping and should really be configured to not accept Telnet connections at all via central access control list (ACL) configurations.

Our Advice

Organizations should review what they have placed on the internet and strive to eliminate the use of Telnet as soon as possible.

ISPs should block Telnet and definitely not use Telnet themselves to administer telecommunications services. This is especially true for the Nordic countries, where only a half-dozen ISPs control the majority of the Telnet exposure space.

Regulators in the Nordics should consider banning the use of Telnet on public internet segments and prevent device manufacturers from distributing devices that allow Telnet to be configured.

Secure Shell (SSH)

It's got "secure" right in its name!

SNAPSHOT

WHAT IT IS:	SSH is usually a secure alternative to Telnet, but it also can wrap virtually any protocol in a warm, comforting blanket of cryptographic security.
HOW MANY:	163,290 discovered nodes
VULNERABILITIES:	As with Telnet, the usual exposures associated with SSH stem from default passwords and password reuse. Also, SSH tends to surface vulnerabilities present in a given operating system's cryptographic libraries.
ADVICE:	Deploy SSH judiciously, and have a system in place for generating and maintaining secure passwords or private keys.
ALTERNATIVES:	There are certainly alternatives to SSH, but it is free, open source, and well-maintained by a network of academic and commercial software developers. It is hard to imagine a reasonable alternative to SSH, especially given that SSH can wrap otherwise insecure protocols.

The Nordics View

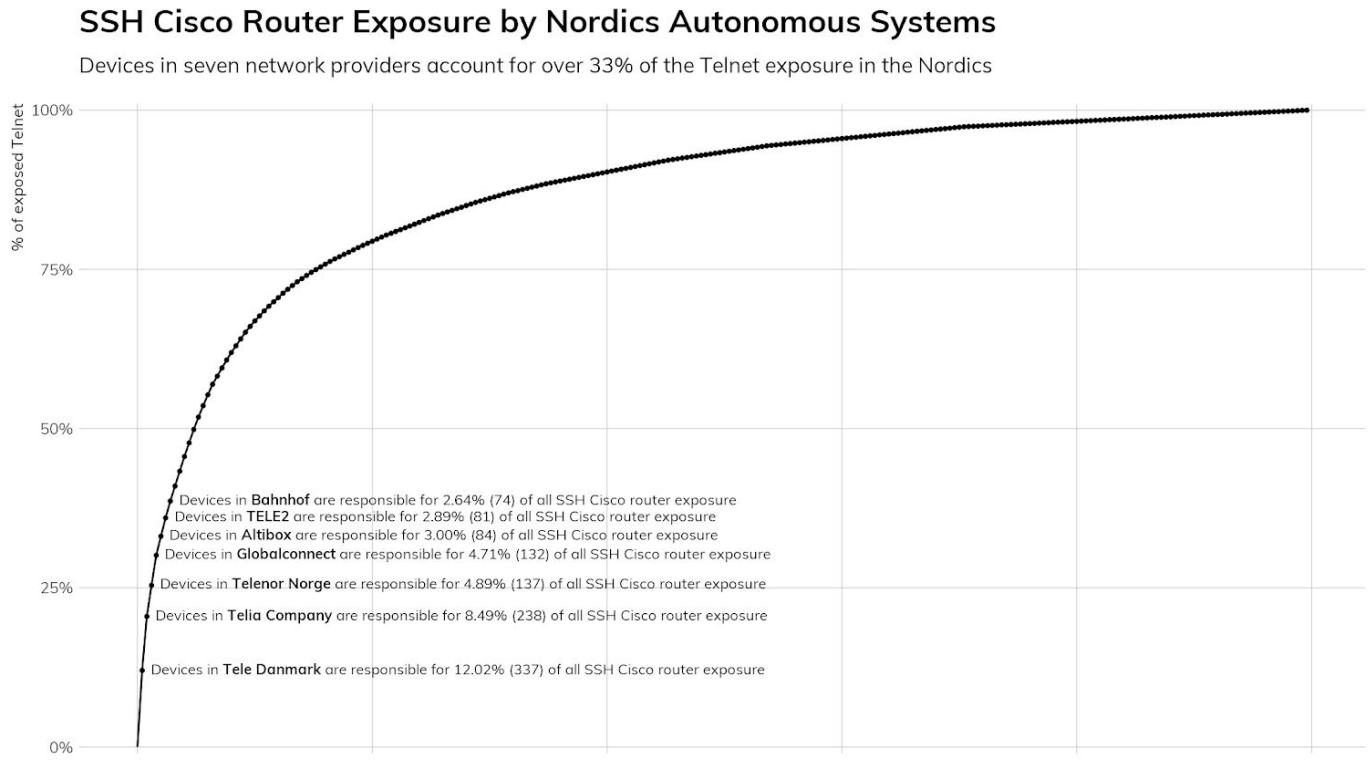
While Telnet exposure fell mostly in ISP and traditional hosting providers, the cloud is where it's at when it comes to SSH exposure. Amazon, UpCloud, and GleSys together make up nearly 25% of discovered SSH services. As noted in the TLDR, SSH can be a great way to provide secure remote access to a system, provided you're using certificate-based access and/or require multi-factor authentication, **and** keep the versions current, which these cloud users clearly are not doing:

OPENSSH VERSION	AMAZON	GLESYS	UPCLOUD
3.6.1p2	0	1	0
3.7.1p2	0	1	0
3.8.1p1	1	0	0
4.2p1	0	4	0
4.3	0	40	2
4.3p2	2	5	1
4.6p1	1	0	0
4.7	0	6	0
4.7p1	1	45	0
5.1	0	4	0
5.1p1	1	37	4
5.2	0	16	0
5.2p1	0	1	0
5.3	12	280	217
5.3p1	1	176	6
5.5	0	3	0
5.5p1	3	174	17
5.6	0	2	0
5.8	0	11	0
5.8p1	1	19	0
5.9	1	0	0
5.9p1	0	243	34
6	0	1	0

OPENSSH VERSION	AMAZON	GLESYS	UPCLOUD
6.0p1	1	398	48
6.1p1	0	3	0
6.2	15	1	0
6.2p2-hpn13v14	0	1	0
6.3	0	1	0
6.4	0	36	1
6.4_hpn13v11	0	1	0
6.5	0	1	0
6.5p1	0	1	0
6.6	0	5	0
6.6p1	0	107	0
6.6p2	0	4	0
6.6.1	23	84	41
6.6.1p1	74	632	269
6.6.1_hpn13v11	0	1	0
6.7	0	1	0
6.7p1	5	520	590
6.7p2	0	1	0
6.9	0	5	0
6.9p1	0	1	0
7	0	2	0
7.1	0	1	0
7.1p2	0	1	0
7.2	0	20	2
7.2p2	855	1,652	1,128
7.3	0	1	0
7.3p1	1	1	0
7.4	6,457	492	1,227
7.4p1	243	666	821
7.5	1	9	6
7.5p1	0	0	1
7.6	4	5	2
7.6p1	3,074	2,792	5,014
7.7	1	5	12
7.7p1	5	0	2
7.8	70	29	75
7.9	34	14	46
7.9p1	44	254	445
8	112	18	217
8.0p1	10	7	2

OPENSSH VERSION	AMAZON	GLESYS	UPCLOUD
8.1	21	16	10
8.1p1	1	3	3
8.2	10	5	8
8.2p1	54	29	16
8.2p2	0	2	0

While exposing SSH on servers is okay, exposing it for internet-based router administration is much less okay. But, there are just over 2,800 Cisco routers across 249 autonomous systems exposing admin access, with high concentrations in Tele Danmark, Telia, and Telenor Norge.



Our Advice

Organizations should strive to have as minimal an SSH footprint as possible, ensure version currency, and mandate certificate and/or multi-factor authentication for sessions. For a clearer picture as to why this is paramount, read the SSH section in the parent NICER report.

Cloud providers should make it next to impossible to run instances with outdated versions of SSH and provide a monitoring and notification service to customers when outdated versions or insecure configurations are detected. Not doing so risks the reputation of the cloud vendor network and potentially provides indirect (free) compute cycles and bandwidth to attackers.

Regulators in the Nordics should encourage the use of SSH over Telnet and provide guidance on safe operating practices for this critical protocol.

Remote Desktop Protocol (RDP)

It's like VNC, but more Microsofty.

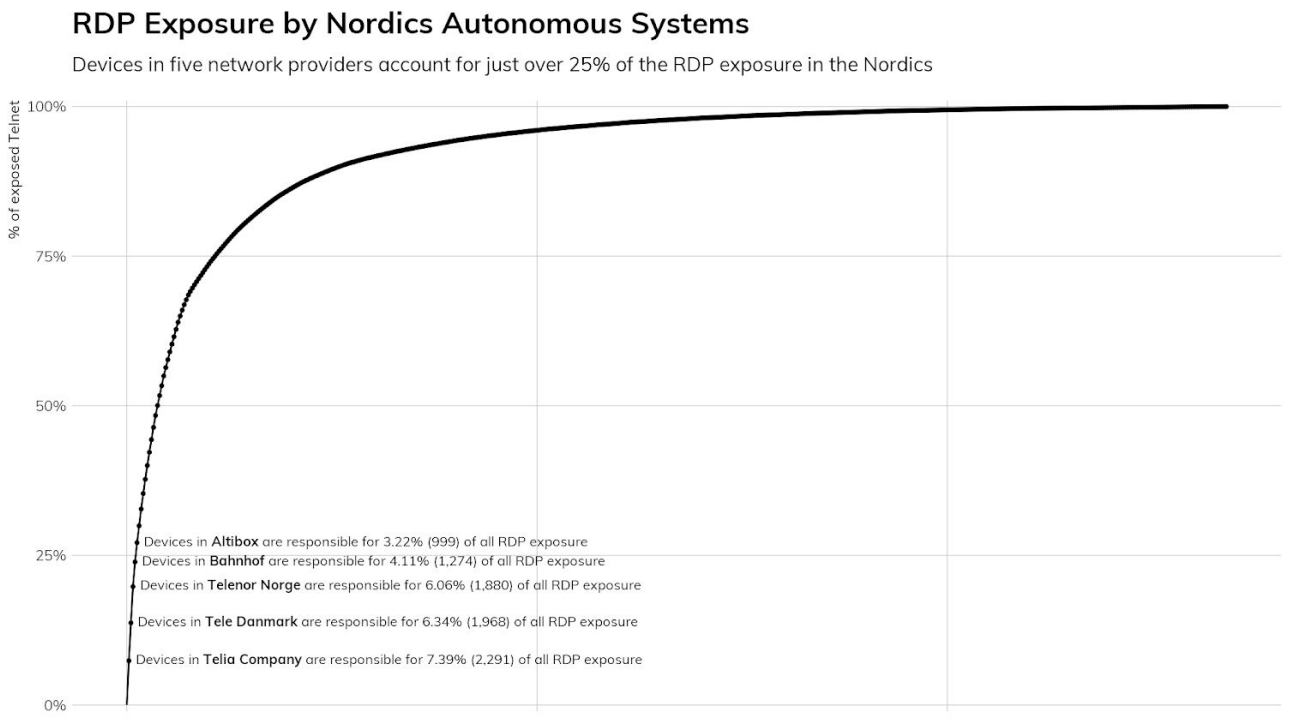
SNAPSHOT

WHAT IT IS:	A proprietary protocol developed by Microsoft for making graphical user interface (GUI) connections from one system to another. The default port is TCP/3389, but it can be hosted on any open port.
HOW MANY:	31,017 discovered nodes
VULNERABILITIES:	Numerous remote code execution issues, including CVE-2019-0708[3] (BlueKeep), which was disclosed by Microsoft in the spring of 2019.
ADVICE:	Place RDP behind a VPN connection if it needs to be "always on." If RDP can be made intermittently available, ensure all nodes exposing RDP are fully patched, hardened to recommended specifications, and utilize multi-factor authentication.
ALTERNATIVES:	This is Microsoft's recommended solution for remotely accessing remote systems. It does what it says on the tin pretty well, so there are no real alternatives. If you need this type of access, follow the guidance in the **Advice** section.

The Nordics View

While Microsoft Remote Desktop provides quick and efficient access to Windows servers within your company's network, it was never truly designed to be exposed directly to the internet and has become one of the most exploited services on the internet. While nearly 95% of Nordic-exposed RDP is using network-level authentication[4]—which helps prevent basic attacks from being successful—just exposing RDP can be dangerous given how easy it is to perform brute force or credential stuffing attacks against these systems.

Unlike Telnet and SSH, RDP is being used across nearly 550 autonomous systems, which makes sense, since many organizations and individuals stand up RDP out of convenience. However, there are some concentrations in a few business- and residential-class ISP networks (versus hosting or cloud providers):



[3] BlueKeep/CVE-2019-0708 <https://attackerkb.com/topics/huQasjoVMS/windows-remote-desktop-rdp-use-after-free-vulnerablility-bluekeep?>

[4] NLA <https://en.wikipedia.org/wiki/Network_Level_Authentication>

Our Advice

Organizations should strongly consider moving RDP systems behind a well-configured and well-maintained virtual private network (VPN). At the time of publication, there are over 15 billion credentials[5] available to attackers, many of which were gathered from phishing attacks and exfiltration of credential stores, so you can't count on a simple username and password combination to successfully keep out attackers.

ISPs and hosting providers should dissuade customers from standing up RDP services and help provide alternative ways to remotely administer systems or access critical applications.

Regulators in the Nordics should provide strong counsel against the use of direct internet RDP connections and identify alternative approaches to graphical remote access to systems.

File Transfer Protocol (FTP)

A confusing data channel negotiation sequence and totally cleartext—what could go wrong?

SNAPSHOT

WHAT IT IS:	FTP was first standardized in RFC 114, and like most protocols of that era, it relies on cleartext exchanges for authentication and data transfer. Traditionally, FTP uses TCP/21 as its control channel, and the client and server negotiate a second channel for the actual data transfer in either "active" or "passive" modes, thus confounding an entire generation of firewall administrators.
HOW MANY:	243,890 discovered nodes (but this may be due to poor network device configurations on the part of some ISPs).
VULNERABILITIES:	The majority of the fingerprinted versions have DoS and auth/unauth RCE-documented vulnerabilities with associated exploit code, and some have documented backdoors.
ADVICE:	All of the above arguments against Telnet apply to FTP. When you discover FTP on a publicly exposed network, you can be fairly certain the organization involved is running on an ancient legacy of public computing and does not enjoy the benefits of a mature security program.
ALTERNATIVES:	Today, there are several useful alternatives to FTP. SFTP is essentially FTP wrapped in SSH, while FTP/S is wrapped in an SSL layer, much like HTTPS. For file transferring in general, SCP and rsync over SSH tunnelling are perfectly delightful solutions, and, of course, HTTPS-based file sharing applications are well established in today's enterprise networks the world over. This is all to say, there is no good reason to stick with this legacy protocol.

[5] https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover

The Nordics View

We did a bit of a double-take when we saw the exposure counts for FTP. While it still is a wildly popular method of file transfer, this is quite a bit of exposure for a region with just under 2 million discovered internet-facing servers/routers/devices. Yet, Telia does provide provide online documentation for using FTP in the context of web-hosting,[6] and Telenor suggests that FTP is the de facto way to upload security camera footage.[7] We mention those two network providers since they account for 56% (122,973) of all the FTP exposure in Nordics networks.

FTP can be difficult to fingerprint if there are "vanilla" username and password prompts provided, but our scans identified quite a few of these exposed servers. One area of concern is the number of network-attached storage (NAS) and multi-function devices directly exposed to the internet:

DEVICE	COUNT
Asus WAP	2,546
QNAP NAS (Turbo Station)	1,830
Synology NAS (DiskStation)	599
Axis Webcam	328
Netgear NAS	298
ZyXEL (Unified Security Gateway)	166
TP-LINK	113
Asus DSL Modem	92
Western Digital NAS (My Book)	73
Synology	64
AVM WAP (FRITZ!Box)	49
Axis	18
APC Power device	13
Lexmark Printer	12
Konica Minolta Printer	11
Sharp Printer (MX Series)	8
ZebraNet Print server	6
Ricoh Multifunction Device	5
Xerox Printer (Phaser)	4
HP Printer (JetDirect)	3
Kyocera Multifunction Device (TASKalfa)	3
Ricoh Multifunction Device (Aficio)	3
Cisco	2
EMC Storage	1
Xerox Printer (WorkCentre)	1

[6] https://www.telia.se/privat/support/info/konfigureraftp
[7] https://www.telenor.no/bedrift/aktuelt/nettverk/holmenkollen-tradlost-nettverk/

These devices rarely receive patches, and QNAP, Synology, and ZyXEL have been favorite targets of attackers, especially in 2020.

The overall counts of distinct, fingerprinted hardware devices (above) and software products (below) add up to ~30% (71,531) of the total discovered FTP nodes—which is still *far too much FTP on the internet.*

DEVICE	COUNT
Pure-FTPd	24,225
ProFTPD Project ProFTPD	12,381
vsFTPd	10,462
Microsoft IIS	7,098
FileZilla FTP Server	5,643
Bftpd Project Bftpd	703
GNU SmbFTPD	663
Rhino Software Serv-U	604
Gene6 FTP Server	201
ZyXEL FTPD	166
Ipswitch WS_FTP	99
tnftpd	95
Washington University WU-FTPD	91
Västgöta-Data AB zFTPServer	51
Multicraft Multicraft	32
vsFTPd Extended	21
ucftpd	18
NcFTP Software NcFTPd Server	17
APC AOS	13
Konica Minolta KM FTPD	11
FTPD	5
HP JetDirect	3
Apple FTP	1
Blue Coat Proxy	1
EFI Fiery Print Server	1
EMC Celerra	1
TBS FTP Server	1

Our Advice

Organizations should never use FTP. It's old, cumbersome, cleartext, and fraught with peril. There are modern ways to efficiently transfer files to and from servers and devices, all supporting encryption.

ISPs and hosting providers should discourage the use of this outdated protocol and offer fast, efficient, and secure alternatives.

Regulators should use FTP as an example of the dangers of using cleartext protocols and ensure companies understand that they face real consequences if their use of this insecure protocol ends up exposing confidential customer or consumer information.

Nordics Vulnerability Exposure

In this focused look at the Nordics, we wanted to examine specifically the types of high- and medium-severity vulnerabilities that appear to be exploitable today over the internet. As in NICER, these vulnerabilities are restricted to only those that we can detect more or less obviously: the vulnerable software is fingerprintable to at least a given vendor and version (anonymously, without credentials); that software at that version is known to have at least one known, public vulnerability that is listed in the CVE dictionary; and that CVE entry has an associated CVSS score.

High-Severity Vulnerabilities

While the CVSS method of scoring vulnerabilities has its challenges,[8] it's the most convenient method we have of expressing the riskiness of a given public vulnerability. For our purposes, a "high-severity" vulnerability is one that scores at 8.5 or higher, and these vulnerabilities nearly all have some kind of remote code execution (RCE) component—a bad guy who exploits these vulnerabilities tends to gain unfettered access to the component affected.

VENDOR	PRODUCT	NUMBER OF SYSTEMS/DEVICES WITH HIGH-SEVERITY VULNERABILITIES
samba	samba	6,149
isc	bind	1,866
proftpd	proftpd	1,650
apache	http_server	1,113
openbsd	openssh	844
microsoft	iis	251
ibm	lotus_domino	37
exim	exim	22
sun	java_system_web_proxy_server	21
apple	cups	16
apache	couchdb	2
novell	groupwise	2

The Samba weaknesses, such as CVE-2012-1182,[9] have working exploits that can result in executing code with root privileges. While the Nordics are not riddled with such systems, there are enough to create a sizable botnet, and each entry point may provide deeper access into backend networks.

[8] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=635185

[9] https://attackerkb.com/topics/u6DlzoLbwe/cve-2012-1182-samba-rce-via-rpc

Similarly, major weakness in ProFTPD, such as CVE-2015-3306,[10] enable virtually complete unauthenticated control over the remote system, especially if it is paired with a PHP-enabled web server.

The overall counts may be small, but they are made up for by the Telnet, SSH, and RDP exposures.

Medium-Severity Vulnerabilities

High-severity vulnerabilities are always the stars of any exploitation story, since they tend to be "easy" to leverage to get control of a given system, but medium-severity vulnerabilities are nothing to sneeze at. These vulnerabilities don't tend to be straight shots at RCE, but they do tend to offer the next best thing for attackers, which is leaking passwords or other confidential material. For example, the Cisco ASA vulnerability CVE-2020-3259[11] is merely a 7.5, but it involves leaking some pretty critical SSL key material, which can lead to a compromise of an entire VPN environment.

VENDOR	PRODUCT	NUMBER OF SYSTEMS/DEVICES WITH HIGH-SEVERITY VULNERABILITIES
apache	http_server	115,479
isc	bind	26,810
openbsd	openssh	13,700
thekelleys	dnsmasq	7,562
samba	samba	6,439
nginx	nginx	2,659
proftpd	proftpd	1,651
squid-cache	squid	1,322
exim	exim	1,248
apache	tomcat	656
microsoft	iis	251
mortbay	jetty	201
caucho	resin	48
ibm	lotus_domino	37
sun	java_system_web_proxy_server	35
microsoft	personal_web_server	34
apple	cups	29
apache	couchdb	21
sun	java_system_web_server	12
libssh	libssh	8
tornadoweb	tornado	8
mailenable	mailenable	6
ipswitch	imail_server	3
novell	groupwise	2
altn	mdaemon	1
netscape	commerce_server	1

[10] https://attackerkb.com/topics/1Qhi2ndx91/cve-2015-3306-proftpd-unauthenticated-remote-read-write
[11] https://attackerkb.com/topics/g0etAbGFCv/cve-2020-3259

The bulk of these medium-severity vulnerabilities enable trivial denial-of-service attacks, with a handful, such as CVE-2013-2249,[12] possibly allowing other remote actions, depending on the configuration.

What's more troubling about this cadre of vulnerabilities (of all severity levels) is the version diversity in components that are fairly trivial to update. Our scans picked up no fewer than 108 distinct versions of Apache Tomcat,[13] a Java application environment that backs many diverse web applications, and 96 separate versions of Apache HTTPD.

VENDOR	PRODUCT	NUMBER OF DISTINCT VERSIONS DISCOVERED
apache	tomcat	108
apache	http_server	96
nginx	nginx	92
samba	samba	87
openbsd	openssh	49
isc	bind	47

Having these old versions exposed to the internet is a signal to attackers that the rest of your infrastructure might be equally as unkempt and make you a more likely target of attacks.

Conclusions

The exposure of the Nordic region is generally better than the overall level of exposure worldwide. Sweden is the highest-ranked country in the region in terms of internet exposure, coming in at 26th most exposed. Meanwhile, Norway was the 45th most exposed, and none of the other countries (Denmark, Faroe Islands, Finland, Greenland, and Iceland) showed up in the top 50 at all.

That said, the preponderance of nearly half a million cleartext FTP servers, along with the tens of thousands of exposed Telnet and RDP servers, ought to be cause for some concern in the region. In order to improve the local online exposure situation, Nordic readers should ensure that whenever a system is open to the internet, it should be:

- **Exposed deliberately.** You meant to expose it versus accidentally exposed it.
- **Configured competently.** The configuration is secure and designed to perform only the necessary tasks.
- **Patched regularly.** You need to make a real effort to keep with current version levels and especially when there are critical vulnerabilities identified. You also need to go out of your way to ensure you can pull patched versions even when your default package repositories stop updating.
- **Monitored mindfully.** You have just increased the attack surface of both yourself/your organization and the internet as a whole; as such, you are inherently responsible for doing your part in the defense of those entities.
- **Assumed attacked.** Researchers aren't the only ones looking for services, and attackers do not have the ethical and legal restrictions we do, so they'll look harder and attack at will. You cannot assume that your services will only receive benign interactions using the methods you outlined in your benign use cases.

Read the Full Report

https://www.rapid7.com/nicer2020/

[12] https://attackerkb.com/topics/Ox3QTCWuJI/cve-2013-2249
[13] https://tomcat.apache.org/