Information Security Report

Confidential patient data freely accessible on the internet

Cyber Resilience Report

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2019-09-16

Contents

1. Executive Summary 3
2. Modus operandi 4
3. Findings 6
   3.1. Vulnerability Analysis 11
   3.2. Web Access 12
4. Attack scenarios and value of data 12
   4.1. Value of the data 13
5. Boundaries of this analysis 14
6. Remediation 15
7. Attachments 15
   7.1. Listings 16

1. Executive Summary

Between mid-July 2019 and early September 2019, Greenbone Networks carried out an analysis of approximately 2,300 medical image archiving systems connected to the public internet. These PACS servers (Picture Archiving and Communication Systems) are used in the healthcare sector to archive images created by radiological processes and to make them available to attending physicians to review. This protocol is known as DICOM (Digital Imaging and Communications in Medicine).

The fact that PACS servers are vulnerable to attack or are accessible is not new information, and there have been a number of reports on this topic in the past. No report, however, has dealt with the breadth and depth of the problem associated with unsecured PACS servers.

Greenbone's analysis shows that several hundred PACS servers worldwide are connected to the public internet without any kind of protection for the personal and medical data stored on them. A not inconsiderable number of these systems even allow access to the individual image data of any patient.

All identified systems disclosed the patient's name, date of birth, date of examination and some medical information about the reason for examination.

Of the 2,300 archive systems worldwide that were analyzed, 590 of them have been identified as accessible on the internet; together they contain over 24 million data records from patients from across 52 countries. There are more than 737 million images linked to this patient data, around 400 million of which are accessible or can be easily downloaded from the internet. In addition, there are 39 systems that allow access to patient data via an unencrypted HTTP Web Viewer, without any protection.

In the UK, approximately 1,500 patient data records are publicly accessible, as well as around 5,000 images associated with these records. In the US, the number is orders of magnitude higher with 13.7 million data sets and 45.8 million images freely accessible on the internet.

As an estimate derived from previous attacks and investigations by various security authorities, the value of this data on the Darknet would probably be in excess of one billion US dollars.

This data could be exploited by attackers for various purposes. These include publishing individual names and images to the detriment of a person's reputation; connecting the data with other Darknet sources to make phishing attacks and social engineering even more effective; reading and automatically processing the data to search for valuable identity information, such as Social Security Numbers, in preparation for identity theft.

This global data leak affects data protection regulations in Europe (GDPR) as well as in the US (HIPAA), and a whole range of legal regulations in other countries. IP addresses or systems from 93 countries and territories were checked.

The following chapters describe, in detail, the analysis procedure, the findings, possible attack scenarios, and ways of remedying them.

A list of files can be found in the appendix. These contain the individual data sets that were used for this security report. These files are made available only upon request and only to organisations with a legitimate interest.

It must be emphasized that no program development or coding was necessary to evaluate this data leak. No exploits were written, unknown/unpublished vulnerabilities were exploited. Also, no complete data sets, nor complete archives were downloaded or saved.

2.Modus operandi

Various sources were used to identify PACS servers worldwide, including the well-known sources Shodan.io and Censys.io. The basic data consisted of a list of about 2,300 IP addresses and port numbers of the DICOM protocol.

The DICOM protocol uses ports 104/TCP and 11112/TCP as standard for communication between DICOM-enabled applications. This involves the loading of image data and patient information into the archive system by imaging devices (X-ray, CT, MRI) and the retrieval of this data for review e.g. by the treating physician.

The DICOM protocol or format is of essential importance in this analysis and is described as follows by the European Commission as:

"DICOM (Digital Imaging and Communications in Medicine) is a standard for handling, storing, printing, and transmitting information in medical imaging. It includes a file format definition and a network communications protocol. The communication protocol is an application protocol that uses TCP/IP to communicate between systems. DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format."

For this security report, only the use case 'reading access' was of interest. A manipulation of image data and the subsequent upload was not investigated.

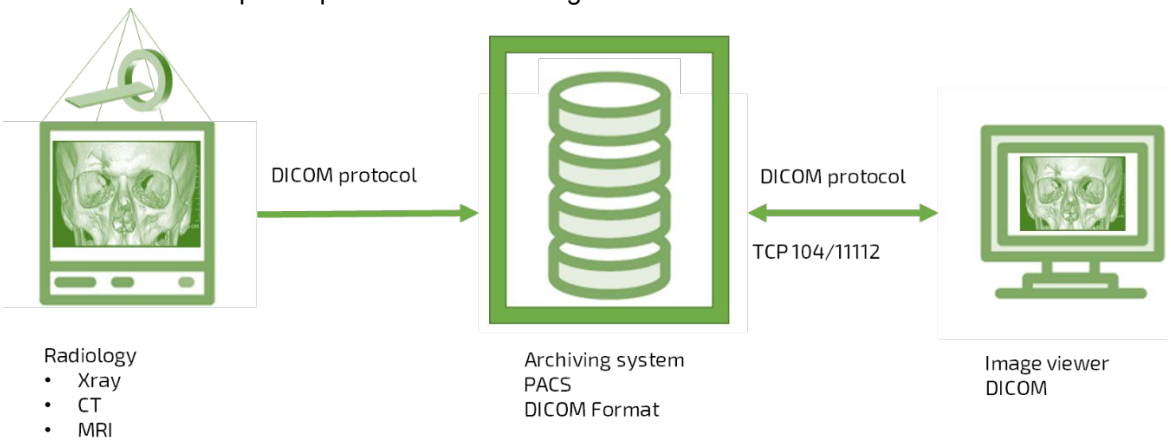


Image 1: Sketched procedures in DICOM protocol / format

In accordance with the CIA triad (Confidentiality Integrity Availability), this report deals only with the confidentiality of the data, which is not guaranteed.

The RadiAnt DICOM Viewer was used to illustrate how easy it is to read this medical data. Other tools were not needed to understand how the data works. The RadiAnt DICOM Viewer was sufficiently documented on the internet to enable even an internet-savvy beginner to configure the application itself. To configure the Viewer, the server parameters IP and Port were required (see Shodan/Censys) and two further specifications, the contents of which were selected completely arbitrarily (AE -title and description).

Once the configuration was complete, the Viewer was used to check whether the PACS was sending data or whether other protective measures were taken (which was the case for around 1,700 of the systems checked).

If no further protective measures were available, the PACS sent the patient data to the Viewer. In addition, the Viewer also allowed the images to be viewed, although there may be a limitation (possibly a question of image compression, which was not subject to analysis).

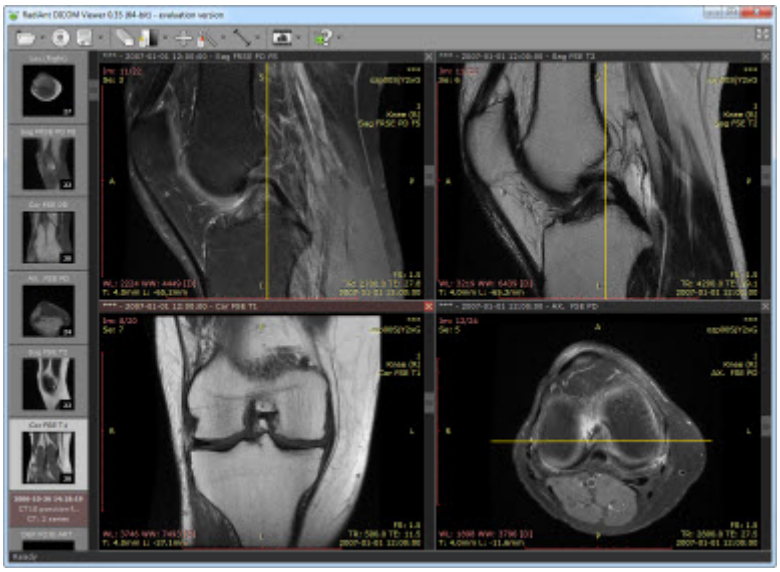


Image 2: RadiAnt DICOM Viewer Content,
Source: https://commons.wikimedia.org/wiki/File:RadiAnt_DICOM_Viewer.jpg

As soon as the Viewer received the data, individual patient data was displayed and counted in a table. This was used for analysis to determine the number of affected patient records.

For each individual data record, there was almost always information on the number of medical images linked to the data record. This listing of all data records was averaged and multiplied by the number of data records to obtain an estimate of the number of images in the archive system.

From the first elements of the list, an entry was randomly selected to verify the actual access to the image data. As soon as a stable data stream in the Viewer indicated that image information was being transferred, this was aborted. In some cases, however, the image transmission was so fast that patient images were also displayed.

The following data points were collected for analysis:

- Number of patient files (called Viewer Studies in DICOM)
- Total number of images on the PACS server
- Data timeliness (e.g. patient data from AUG/SEP 2019)
- Access to images allowed/possible
- Human or veterinary medical archives

In the further course of the analysis, the IP addresses were also scanned with a vulnerability scan and added as an additional data point (high severity vulnerabilities).

The evaluation of the vulnerability scan revealed some indications of compromising systems. This information was also added as a data point.

In addition to the actual analysis, page findings were checked e.g. references to freely downloadable DICOM archives or web apps that allow uncontrolled access to patient data.

Further details can be found in Chapter 3, "Findings".

3.Findings

The analysis of the systems resulted in the following sums and detailed findings.

In total, around 24.3 million data records can be retrieved worldwide, the vast majority of which list the following personal data:

- First name and surname
- Date of birth
- Date of examination
- Scope of the investigation
- Type of imaging procedure
- Attending physician
- Institute/clinic
- Number of generated images

In Europe, this information is protected by GDPR and by HIPAA (Health Insurance Portability and Accountability Act) in the US. There are also corresponding regulations in other countries, e.g.

- Republic South Africa: Protection of Personal Information Act (POPI Act)
- Brazil: Lei Geral de Proteção de Dados Pessoais (LGPD)
- India: Information Technology Act 2000, Data Privacy Rules
- Turkey: Personal Data Protection Law no. 6698

Two further totals result from the individual data points mentioned above. The number of images linked to the 24.3 million data sets amounts to an estimated 733.5 million, of which an estimated 399.5 million images (from the more than 700 million) can be accessed, displayed and downloaded.

The sum of these data leaks of unprotected patient data available on the internet is one of the largest data glitches worldwide to date. 52 countries around the world are affected, including all leading economic nations and the most populous countries in the world.

The countries affected include:

Argentina, Australia, Brazil, Canada, China, Egypt, France, Germany, India, Iran, Italy, Japan, Korea, Mexico, the Netherlands, Russia, South Africa, Spain, Switzerland, Turkey, the United Kingdom, and the United States of America.

The following figures apply to selected countries in Europe:

Image 3: Figures in Europe

The number of systems affected is shown in the table below:

Country	CH	CZ	DE	ES	FR	IT	NL	UK
Systems	2	2	6	1	7	10	4	5

For North America, the data is as follows:

Image 4: Figures in North America

The number of systems affected is shown in the table below:

Countries	CA	MX	US
Systems	5	10	187

The numbers for South America look like this:

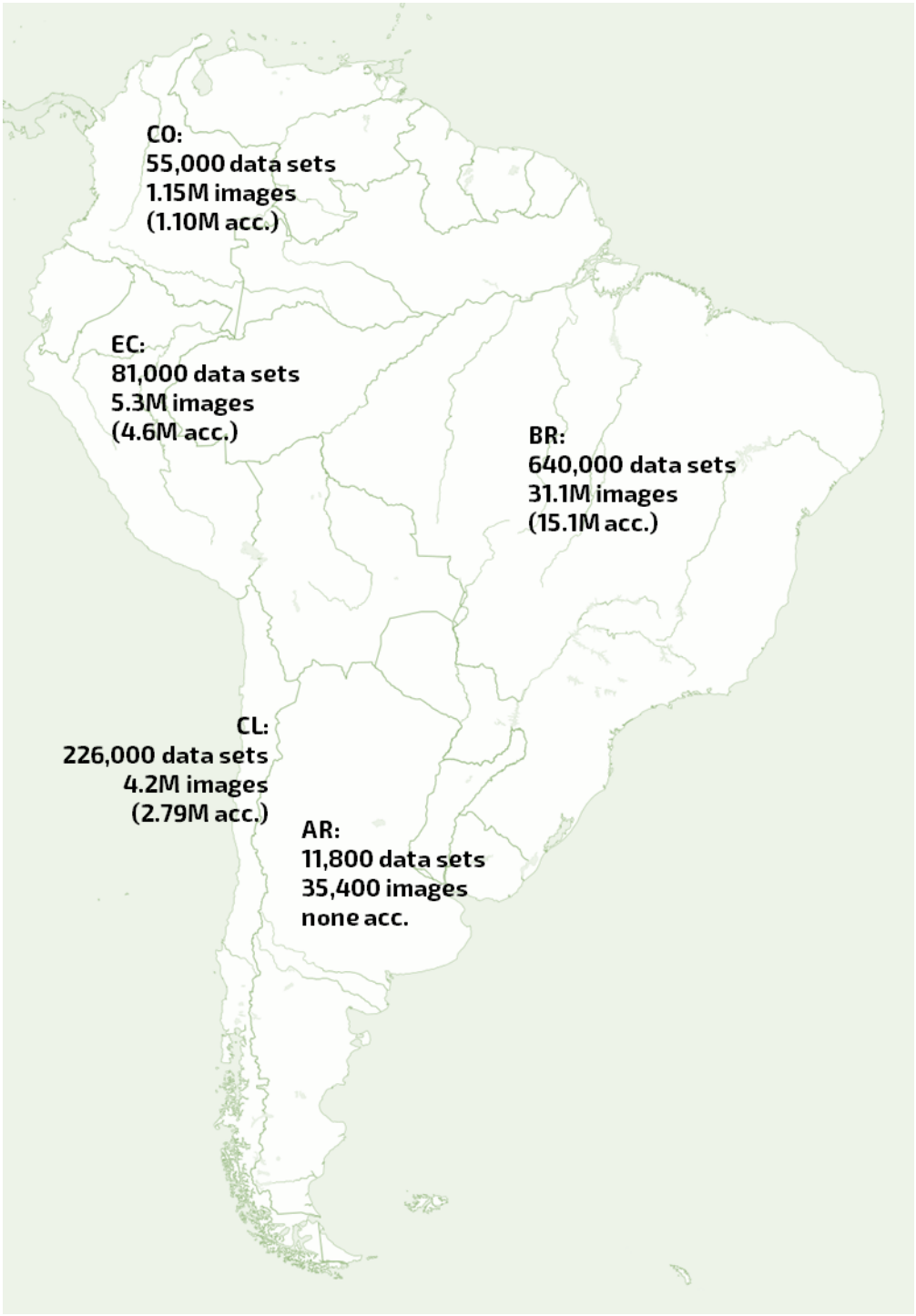


Image 5: Figures in South America

The number of systems affected is shown in the table below:

Countries	AR	BR	CL	CO	EC
Systems	10	34	18	8	19

The following map shows the results for Asia:

Image 6: Figures in Asia

The number of systems affected is shown in the table below:

Countries	CN	IN	JP	RU	TR
Systems	14	96	3	5	36

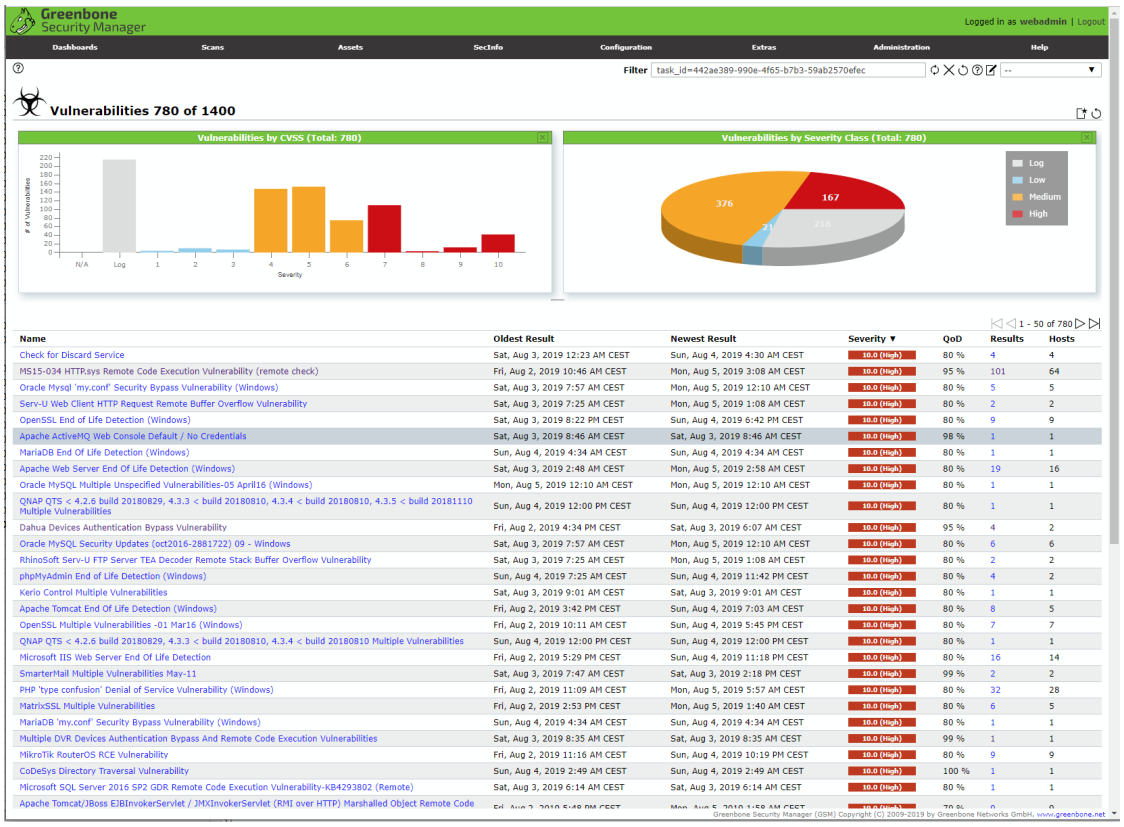
In South Africa and Australia::

30 archive systems in South Africa and a further 6 systems in Australia are also affected.

3.1. *Vulnerability Analysis*

In addition, a number of vulnerabilities, some several years old, were identified on the audited systems.

The screenshot below shows more information:



In total, Greenbone has identified more than 10,000 vulnerabilities on the systems. Just over 2,000 of these are catalogued as 'high severity' and this category includes more than 500 vulnerabilities with the highest severity, CVSS 10.0.

These CVSS 10.0 vulnerabilities most often include vulnerable web applications and databases, which are also common targets for hackers.

Further details of the vulnerability analysis can be provided (the report is 300MB in size).

Further analysis showed that individual systems also had Indicators of Compromise. We did not investigate this aspect further at this time.

3.2. *Web Access*

Beside the archive systems that can be addressed and queried without protection via the DICOM protocol, our research also found other ways in which medical data was easily accessible:

- We found 31 systems that allowed direct access to patient data via a DICOM Web Viewer. This access was possible without authentication, and in most of these 31 systems, the data was transmitted via HTTP, i.e. unencrypted in plain text. The web viewers also offered a file upload that we did not investigate further. Whether security mechanisms were installed here remains questionable.

- Seven systems offered complete DICOM archives as downloads via HTTP, totaling about 108 gigabytes of data. The archives themselves were not downloaded or examined.

- Six server systems offered an unencrypted FTP service with anonymous access, i.e. without password or other protection. Here, patient data could also be found directly on at least one system.

- One system was configured in a way that we did not observe for an extended period of time. This system displayed the files of the DICOM archive via directory listing in the web browser. The respective images could be easily downloaded.

4. Attack scenarios and value of data

Since it is personal data that is accessible, the possible attack scenarios are manifold, including:

- Social Engineering
- Spear Pishing / Whaling
- Business Email Compromise

In addition, the intersection of this data with other sources, such as other already leaked data sets, could be used to prepare for even more targeted attacks. Extortion attempts are also conceivable, as is identity theft, particularly in the US where some of the data contains patients' Social Security Numbers.

The US Department of Health (HHS) has listed a number of scenarios that exploit patient data:

"Medical Identity Theft"

The use of another person's medical information to obtain a medical service, which includes:

- Medical prescriptions
- Surgery or other medical treatment
- Counterfeit settlements against health insurers

“Weaponizing of Medical Data”

The use of sensitive medical data to threaten, extort, or influence individuals, in order to:

- Extort money
- Disparage someone by false or real additional data
- Exploit individuals who are in the public eye
  (In our research, we did not search for high-profile names within in the data)

“Financial Fraud”

The use of Personally Identifiable Information (PII) contained in electronic medical records to create credit card or bank profiles to facilitate financial fraud. This could be done through:

- The financial information on patient data that medical service providers often store (we have seen billing information references in the data)
- The loans and credit lines that are often linked to health data found in patient files.
- Tax fraud through false billing

“Cyber Campaigns”

The use of medical data as complementary data in future hacking campaigns, including:

- Contact information that can be used for phishing or scams (CEO fraud)
- Credential/authentication information that can be used for a privilege escalation
  (We have not searched for such information in the data)

Within the mass of data and personal information, a number of groups are particularly vulnerable as the exploitation of their data can remain unnoticed for years. These include:

- Children and adolescents whose data is used for identity theft. These can be easily identified in the data found by the date of birth.
- The elderly, combined with the assumption that they are an easier target ("age-associated financial vulnerability"). This group can be easily identified, for example by their date of birth or by the name of the institute found in the data (e.g. "Senior Care").
- Deceased persons or those presumed dead. Based on the date of birth, data is filtered for persons in old age. Here the expected detection rate is very low.

4.1. *Value of the data*

In the course of the analysis, the question arose over how much this data could be worth on the Dark web. An exact statement is difficult to make, but there are some clues for an approximation.

In April 2019, the Department of Health and Human Services (HHS) in the US published an Intelligence Briefing Update. In it, the average value of an Electronic Health Record (EHR) was given as 250 US dollars and the maximum value as 1,000 US dollars.

A comparison with the 18 characteristics mentioned in the HIPAA (see above) in an extensive EHR, showed that the accessible data definitely contained 7 of these characteristics, with another 7

characteristics very likely to have been present, and a further 4 which were very unlikely to be present (see appendix).

On this basis, an approximate value of 50 US dollars per data set is to be assumed, which leads to a total value of unprotected retrievable data of about 1.2 billion US dollars.

This value is certainly not recoverable all at once and not every record will be tradable for $50. However, this sum shows the motivation with which an attacker could search for this data and would most likely do so with more technical effort.

5. Boundaries of this analysis

As part of this investigation, we have identified three areas in which no further investigation has been made. However, according to initial considerations, these areas would be worth a more in-depth review:

1. **Neighbor analysis:**
   The open PACS servers found are part of a medical/clinical process. This means that they communicate within a network of IP-enabled devices via the DICOM protocol. A network scan in the address area of the respective system could reveal further worthwhile targets for an attacker.

   An attacker can safely assume that the security on these neighbor systems also does not comply with current standards, analogous to the PACS server already found.

2. **DICOM brute force:**
   Our analysis showed that a number of systems respond to a "DICOM Ping" (CSP-ECHO), but not to data queries. This is probably due to settings in the AE titles or descriptions that prevent an open query. A review of the DICOM protocol shows that there are no restrictions on the number of attempts to query a system in the protocol. Here a brute force attack would be conceivable, so that further systems disclose data.

   Such scripting was not part of the analysis.

3. **File upload:**
   The DICOM protocol contains methods to upload files to a PACS server (see “Web Access” above). It was not part of our analysis whether this feature could be exploited for an attack on the system (although we estimate that it is possible)). If this were to happen, it would be possible for hackers to gain access to the inner network of medical facilities.

4. **Image manipulation**:
   This attack scenario has already been investigated by Israeli security researchers[1].

[1] https://arxiv.org/pdf/1901.03597.pdf

6.Remediation

Since this is a faulty configuration of the infrastructure and the PACS server, rather than a software vulnerability, there are also possibilities for remedying or eliminating the issue:

- Access Control Lists (ACLs) for IP-addresses and/or port filters
- Access control through the implementation of AAA systems
- VPN access for selected persons/institutions
- Detailed configuration of AE titles

These measures could make accessing the systems more difficult, or prevent access altogether. In doing so, however, it is important to consider which authorized authorities require access to the data, such as hospital associations or general practitioners.

Each individual case will have a limit to the available solutions. However, according to our observations, there is no case in which a higher degree of security would not be worthwhile.

A comprehensive and repeated inventory of IT systems and their vulnerabilities within an organization is the best way to uncover such flawed configurations.

7.Attachments

The following documents about the details are provided only upon request and only to organizations with legitimate interest. These include in particular the data protection authorities of the countries concerned, who can contact security@greenbone.net .

- File „DICOM details per system”
- File „PACS Server free web access”

7.1. *Listings*

Results sorted by country (alphabetical, ascending A-Z):

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
Albania	1	200	1.000	-	-
Anguilla	1	2.972	44.850	-	-
Argentina	10	11.824	25.472	-	-
Australia	6	49.922	2.596.469	2.496.260	-
Barbados	1	14	2.800	-	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Brazil	34	643.892	31.110.131	15.141.864	4
Bulgaria	2	27.058	40.977	40.977	-
Canada	5	117.425	6.019.030	980.500	-
Chile	18	226.886	4.218.279	2.794.898	3
China	14	279.928	4.882.722	376.905	-
Colombia	8	55.345	1.155.195	1.114.602	1
Costa Rica	1	3.202	12.808	12.808	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Czech Republic	2	97.997	674.686	-	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Egypt	2	827	124.130	124.130	-
France	7	47.662	5.275.222	2.668.170	-
Germany	6	15.310	2.859.595	1.394.845	-
Greece	2	10.211	2.557.600	2.557.600	-
Guatemala	4	13.012	1.039.241	1.039.241	2
India	96	627.777	105.941.300	104.120.549	6
Iran	2	118.692	1.903.384	1.903.384	-
Italy	10	102.893	5.843.319	1.174.600	-
Japan	3	10.498	1.725.280	1.719.280	-
Kenya	1	243	14.580	-	-
Korea	2	26.256	86.277	-	1
Malaysia	3	19.922	1.195.320	1.195.320	-
Mexico	10	23.590	965.495	195.475	2
Netherlands	3	11.270	113.408	113.408	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Paraguay	1	22.355	1.676.625	-	-
Peru	2	1.377	177.050	500	1
Portugal	3	5.766	1.581.101	1.581.100	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Romania	1	67	737	-	-
Russian Federation	5	9.858	887.042	25.000	-
Sao Tome and Principe	1	13.402	160.824	-	-
Serbia	1	30.484	15.242.000	15.242.000	-
Slovakia	1	127.636	382.908	-	-
South Africa	30	2.338.112	38.941.118	4.093.500	-
Spain	1	17.662	52.986	-	-
Switzerland	2	1.541	231.840	231.840	1
Thailand	8	433.008	433.895	426.773	-
Turkey	36	4.924.141	179.533.940	178.283.858	-
Ukraine	1	1.139	199.325	199.325	-
United Kingdom	6	1.571	13.335	5.070	-
United States	187	13.700.499	303.126.601	45.870.508	15
Uzbekistan	1	35.475	886.875	886.875	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Vietnam	1	1.471	1.471	-	-

Results sorted by systems (number, descending):

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
India	96	627.777	105.941.300	104.120.549	6
Turkey	36	4.924.141	179.533.940	178.283.858	-
Brazil	34	643.892	31.110.131	15.141.864	4
South Africa	30	2.338.112	38.941.118	4.093.500	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Chile	18	226.886	4.218.279	2.794.898	3
China	14	279.928	4.882.722	376.905	-
Argentina	10	11.824	25.472	-	-
Italy	10	102.893	5.843.319	1.174.600	-
Mexico	10	23.590	965.495	195.475	2
Colombia	8	55.345	1.155.195	1.114.602	1
Thailand	8	433.008	433.895	426.773	-
France	7	47.662	5.275.222	2.668.170	-
Australia	6	49.922	2.596.469	2.496.260	-
Germany	6	15.310	2.859.595	1.394.845	-
United Kingdom	6	1.571	13.335	5.070	-
Canada	5	117.425	6.019.030	980.500	-
Russian Federation	5	9.858	887.042	25.000	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Japan	3	10.498	1.725.280	1.719.280	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Netherlands	3	11.270	113.408	113.408	-
Portugal	3	5.766	1.581.101	1.581.100	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Bulgaria	2	27.058	40.977	40.977	-
Czech Republic	2	97.997	674.686	-	-
Egypt	2	827	124.130	124.130	-
Greece	2	10.211	2.557.600	2.557.600	-
Iran	2	118.692	1.903.384	1.903.384	-
Korea	2	26.256	86.277	-	1
Peru	2	1.377	177.050	500	1
Switzerland	2	1.541	231.840	231.840	1
Albania	1	200	1.000	-	-
Anguilla	1	2.972	44.850	-	-
Barbados	1	14	2.800	-	-
Costa Rica	1	3.202	12.808	12.808	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Kenya	1	243	14.580	-	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Paraguay	1	22.355	1.676.625	-	-
Romania	1	67	737	-	-
Sao Tome and Principe	1	13.402	160.824	-	-
Serbia	1	30.484	15.242.000	15.242.000	-
Slovakia	1	127.636	382.908	-	-
Spain	1	17.662	52.986	-	-
Ukraine	1	1.139	199.325	199.325	-
Uzbekistan	1	35.475	886.875	886.875	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Vietnam	1	1.471	1.471	-	-

Results sorted by records (number, descending):

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
Turkey	36	4.924.141	179.533.940	178.283.858	-
South Africa	30	2.338.112	38.941.118	4.093.500	-
Brazil	34	643.892	31.110.131	15.141.864	4
India	96	627.777	105.941.300	104.120.549	6
Thailand	8	433.008	433.895	426.773	-
China	14	279.928	4.882.722	376.905	-
Chile	18	226.886	4.218.279	2.794.898	3
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Slovakia	1	127.636	382.908	-	-
Iran	2	118.692	1.903.384	1.903.384	-
Canada	5	117.425	6.019.030	980.500	-
Italy	10	102.893	5.843.319	1.174.600	-
Czech Republic	2	97.997	674.686	-	-
Ecuador	19	81.363	5.308.881	4.621.285	2
Colombia	8	55.345	1.155.195	1.114.602	1
Australia	6	49.922	2.596.469	2.496.260	-
France	7	47.662	5.275.222	2.668.170	-
Uzbekistan	1	35.475	886.875	886.875	-
Serbia	1	30.484	15.242.000	15.242.000	-
Bulgaria	2	27.058	40.977	40.977	-
Korea	2	26.256	86.277	-	1
Mexico	10	23.590	965.495	195.475	2
Paraguay	1	22.355	1.676.625	-	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Spain	1	17.662	52.986	-	-
Germany	6	15.310	2.859.595	1.394.845	-
Netherlands Antilles	1	13.992	209.880	209.880	-
Sao Tome and Principe	1	13.402	160.824	-	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Argentina	10	11.824	25.472	-	-
Netherlands	3	11.270	113.408	113.408	-
Japan	3	10.498	1.725.280	1.719.280	-
Greece	2	10.211	2.557.600	2.557.600	-
Russian Federation	5	9.858	887.042	25.000	-
Portugal	3	5.766	1.581.101	1.581.100	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Cyprus	1	3.459	1.124.175	1.124.175	-
Costa Rica	1	3.202	12.808	12.808	1
Anguilla	1	2.972	44.850	-	-
United Kingdom	6	1.571	13.335	5.070	-
Switzerland	2	1.541	231.840	231.840	1
Vanuatu	1	1.512	1.512	1.512	-
Vietnam	1	1.471	1.471	-	-
Peru	2	1.377	177.050	500	1
Ukraine	1	1.139	199.325	199.325	-
Egypt	2	827	124.130	124.130	-
Kenya	1	243	14.580	-	-
Albania	1	200	1.000	-	-
Venezuela	1	76	1.140	1.140	-
Romania	1	67	737	-	-
Barbados	1	14	2.800	-	-

Results sorted by linked images (number, descending):

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
United States	187	13.700.499	303.126.601	45.870.508	15
Turkey	36	4.924.141	179.533.940	178.283.858	-
India	96	627.777	105.941.300	104.120.549	6
South Africa	30	2.338.112	38.941.118	4.093.500	-
Brazil	34	643.892	31.110.131	15.141.864	4
Serbia	1	30.484	15.242.000	15.242.000	-
Canada	5	117.425	6.019.030	980.500	-
Italy	10	102.893	5.843.319	1.174.600	-
Ecuador	19	81.363	5.308.881	4.621.285	2
France	7	47.662	5.275.222	2.668.170	-
Puerto Rico	23	205.691	4.921.604	4.921.604	-
China	14	279.928	4.882.722	376.905	-
Chile	18	226.886	4.218.279	2.794.898	3
Germany	6	15.310	2.859.595	1.394.845	-
Australia	6	49.922	2.596.469	2.496.260	-
Greece	2	10.211	2.557.600	2.557.600	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Iran	2	118.692	1.903.384	1.903.384	-
Japan	3	10.498	1.725.280	1.719.280	-
Paraguay	1	22.355	1.676.625	-	-
Portugal	3	5.766	1.581.101	1.581.100	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Colombia	8	55.345	1.155.195	1.114.602	1
Cyprus	1	3.459	1.124.175	1.124.175	-
Guatemala	4	13.012	1.039.241	1.039.241	2
Mexico	10	23.590	965.495	195.475	2
Russian Federation	5	9.858	887.042	25.000	-
Uzbekistan	1	35.475	886.875	886.875	-
Czech Republic	2	97.997	674.686	-	-
Thailand	8	433.008	433.895	426.773	-
Slovakia	1	127.636	382.908	-	-
Switzerland	2	1.541	231.840	231.840	1
Netherlands Antilles	1	13.992	209.880	209.880	-
Ukraine	1	1.139	199.325	199.325	-
Peru	2	1.377	177.050	500	1
Sao Tome and Principe	1	13.402	160.824	-	-
Egypt	2	827	124.130	124.130	-
Netherlands	3	11.270	113.408	113.408	-
Korea	2	26.256	86.277	-	1
Spain	1	17.662	52.986	-	-
Anguilla	1	2.972	44.850	-	-
Bulgaria	2	27.058	40.977	40.977	-
Argentina	10	11.824	25.472	-	-
Kenya	1	243	14.580	-	-
United Kingdom	6	1.571	13.335	5.070	-
Costa Rica	1	3.202	12.808	12.808	1
Barbados	1	14	2.800	-	-
Vanuatu	1	1.512	1.512	1.512	-
Vietnam	1	1.471	1.471	-	-
Venezuela	1	76	1.140	1.140	-
Albania	1	200	1.000	-	-
Romania	1	67	737	-	-

Results sorted by retrievable images (number, descending):

Country	Systems allowing unprotected access via DICOM	Studies	Images	Image access	Systems allowing unprotected Web/FTP Access/Directory Listing
Turkey	36	4.924.141	179.533.940	178.283.858	-
India	96	627.777	105.941.300	104.120.549	6
United States	187	13.700.499	303.126.601	45.870.508	15
Serbia	1	30.484	15.242.000	15.242.000	-
Brazil	34	643.892	31.110.131	15.141.864	4
Puerto Rico	23	205.691	4.921.604	4.921.604	-
Ecuador	19	81.363	5.308.881	4.621.285	2
South Africa	30	2.338.112	38.941.118	4.093.500	-
Chile	18	226.886	4.218.279	2.794.898	3
France	7	47.662	5.275.222	2.668.170	-
Greece	2	10.211	2.557.600	2.557.600	-
Australia	6	49.922	2.596.469	2.496.260	-
Bolivia	2	4.361	2.174.013	2.174.000	-
Iran	2	118.692	1.903.384	1.903.384	-
Japan	3	10.498	1.725.280	1.719.280	-
Portugal	3	5.766	1.581.101	1.581.100	-
Germany	6	15.310	2.859.595	1.394.845	-
Malaysia	3	19.922	1.195.320	1.195.320	-
Italy	10	102.893	5.843.319	1.174.600	-
Cyprus	1	3.459	1.124.175	1.124.175	-
Colombia	8	55.345	1.155.195	1.114.602	1
Guatemala	4	13.012	1.039.241	1.039.241	2
Canada	5	117.425	6.019.030	980.500	-
Uzbekistan	1	35.475	886.875	886.875	-
Thailand	8	433.008	433.895	426.773	-
China	14	279.928	4.882.722	376.905	-
Switzerland	2	1.541	231.840	231.840	1
Netherlands Antilles	1	13.992	209.880	209.880	-
Ukraine	1	1.139	199.325	199.325	-
Mexico	10	23.590	965.495	195.475	2
Egypt	2	827	124.130	124.130	-
Netherlands	3	11.270	113.408	113.408	-
Bulgaria	2	27.058	40.977	40.977	-
Russian Federation	5	9.858	887.042	25.000	-
Costa Rica	1	3.202	12.808	12.808	1
United Kingdom	6	1.571	13.335	5.070	-
Vanuatu	1	1.512	1.512	1.512	-
Venezuela	1	76	1.140	1.140	-
Peru	2	1.377	177.050	500	1
Paraguay	1	22.355	1.676.625	-	-
Czech Republic	2	97.997	674.686	-	-
Slovakia	1	127.636	382.908	-	-
Sao Tome and Principe	1	13.402	160.824	-	-
Korea	2	26.256	86.277	-	1
Spain	1	17.662	52.986	-	-
Anguilla	1	2.972	44.850	-	-
Argentina	10	11.824	25.472	-	-
Kenya	1	243	14.580	-	-
Barbados	1	14	2.800	-	-
Vietnam	1	1.471	1.471	-	-
Albania	1	200	1.000	-	-
Romania	1	67	737	-	-

HIPAA Characteristics for Personal Health Information:

Characteristic	**Included?**
Patient name	Yes
Dates (birth, treatment, death)	Yes
Physical addresses	No
Fax numbers	Likely
Social security numbers	Yes
certificate/license numbers	No
phone numbers	Likely
full face photos/other pictures	Yes
URLs/web addresses	Likely
E-mail addresses	Likely
health plan beneficiary information	Likely
Internet Protocol (IP) addresses	Yes
medical record #s	Yes
device identifiers and serial #s	Likely
biometric (finger, voice, etc.) info	No
account numbers	Likely
vehicle identification information	No
Other uniquely identifying info	Yes