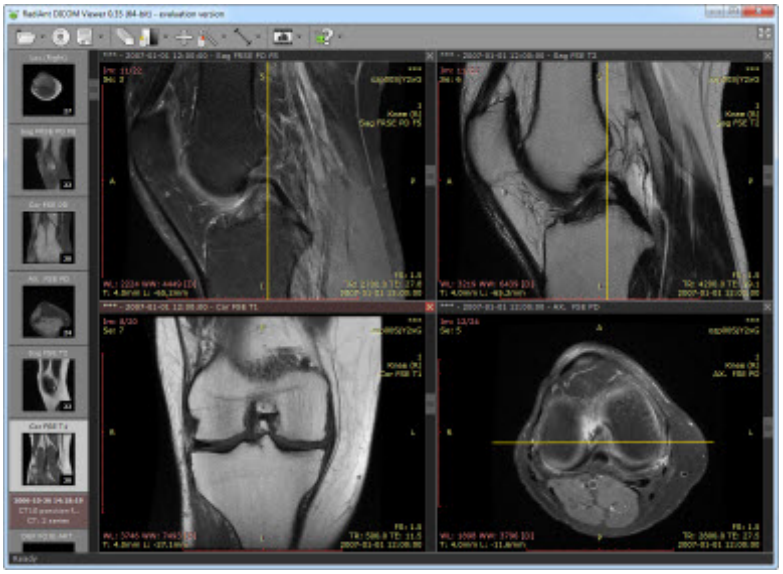
Help Net Security
November 20, 2019

1.19 billion confidential medical images available on the internet

1.19 billion confidential medical images are now freely available on the internet, according to Greenbone's research into the security of Picture Archiving and Communication Systems (PACS) servers used by health providers across the world to store images of X-rays as well as CT, MRI and other medical scans.



US: 786 million medical images identified

That's a 60% increase from the finding between July and September 2019, and includes details of patient names, reason for examination, date of birth, and ID cards in some cases.

Amongst the 786 million medical images identified in the US, which had the largest increase in new data sets discovered, Social Security Numbers were included on some of the images, as well as some sets which listed details pertaining to military personnel IDs from the Department of Defense.

Overall, 129 new easily accessible archiving systems and data from nine additional countries have been discovered. Also, the number of images freely available on the internet had increased

most significantly in the US, India, South Africa, Brazil and Ecuador.

Missing controls

Proper controls, such as HIPAA in the US, were largely missing. In total, the number of data records which are accessible online without any level of protection has doubled, from 4.4 million to 9 million, and the number of images now accessible or easily downloadable via the internet is 370 million.

Conversely, 172 PACS servers, including all systems from 11 countries including the UK, Germany, Thailand and Venezuela, had in fact been taken completely offline and the patient data was no longer accessible via the internet.

Addressing the situation

Dirk Schrader, cyber resilience architect at Greenbone Networks said: “Whilst some countries have taken swift action to address the situation and have removed all accessible data from the internet, the problem of unprotected PACS systems across the globe only seems to be getting worse. In the US especially, sensitive patient information appears to be free-flowing and is a data privacy disaster waiting to happen.

“When we carried out this second review, we didn’t expect to see more data than before and certainly not to have continued access to the ones we had already identified. There certainly is some hope in the fact that a number of countries have managed to get their systems off the internet so quickly, but there is much more work to be done.”

More about

cybersecurity | data security | Europe | Greenbone Networks | healthcare | medical data | privacy | report | USA

Share this

Featured news

December 2019 Patch Tuesday forecast: Make sure to deploy year-end updates

The hidden risks of cryptojacking attacks

Review: Cyber Smart

Nearly half of consumers worry about being tricked by fraudsters this holiday season

Top compliance and risk management challenges for financial organizations

Exploring the proper use of pseudonymisation related to personal data

G Suite admins get restricted security code option

Avoiding the next breach: Four tips for securing your apps

The rise of continuous crowdsourced security testing for compliance

2020 predictions: Rising complexity of managing digital risk

CPoC: New data security standard for contactless payments

How do SMBs plan to improve their security posture in 2020?

The hidden risks of cryptojacking attacks

Review: Cyber Smart

Avoiding the next breach: Four tips for securing your apps

How DNS filtering works and why businesses need it

Supply chain examination: Planning for vulnerabilities you can't control

Spot light **Review: Cyber Smart**

What's new

Review: Cyber Smart

Nearly half of consumers worry about being tricked by fraudsters this holiday season

The hidden risks of cryptojacking attacks

December 2019 Patch Tuesday forecast: Make sure to deploy year-end updates

Top compliance and risk management challenges for financial organizations

Exploring the proper use of pseudonymisation related to personal data

Don't miss

December 2019 Patch Tuesday forecast: Make sure to deploy year-end updates

The hidden risks of cryptojacking attacks

Review: Cyber Smart

N
w
b
s

HELPNETSECURITY

Follow us

- Features
- News
- Expert Analysis
- Reviews
- Events
- Whitepapers
- Industry news
- Newsletters
- Twitter

IN CASE YOU'VE MISSED IT

- 5G IoT security: Opportunity comes with risks
- Preventing insider threats, data loss and damage through zero trust
- Hackers helping communities: Leveraging OSINT to find missing persons
- Your supplier's BEC problem is your BEC problem

(IN)SECURE Magazine ISSUE 63 (September 2019)

- Identifying evasive threats hiding inside

the network

- Inside the NIST team working to make cybersecurity more user-friendly
- Report: Black Hat USA 2019
- Healthcare's blind spot: Unmanaged IoT and medical devices

Read online