Picture Archiving Communication Systems (PACS) Vulnerability

Executive Summary

Picture Archiving Communication Systems (PACS) are widely used by hospitals, research institutions, clinics and small healthcare practices for sharing patient data and medical images. In 2019, researchers disclosed a vulnerability in these systems that if exploited could potentially expose patient data. This is truly concerning due to the ability for Vulnerable PACS servers to easily be discovered via simple open source scanning tools. If left unpatched these systems can expose patient records to unauthorized access. There continues to be a number of unpatched PACs servers visible and HC3 is once again recommending that entities patch their systems immediately.

Background

PACS was developed to assist the transition from analog to digital storage for medical images. PACS servers obtain images such as Ultrasound, CT, MRI and radiography and store them into the Digital Imaging and Communications in Medicine (DICOM) format. The use of the DICOM standard introduces an ability to insert malicious code into imaging files. In early September 2019, researchers identified thousands of vulnerable PACS servers within the US Healthcare sector.

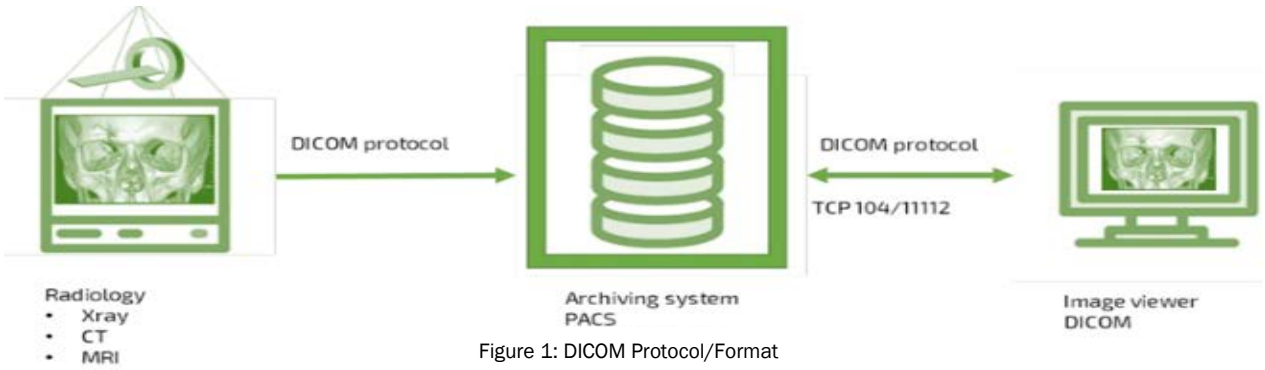

Figure 1: DICOM Protocol/Format

Analysis

Vulnerable PACS servers face additional exposure when directly connected to the internet without a firewall, virtual private network (VPN) or secure password. These vulnerabilities range from known default passwords, hardcoded credentials and lack of authentication within third party software. Successful exploitation of these vulnerabilities can expose patients' medical data, including patient names, examination dates, images, physician names, dates of birth, procedure types, procedure locations and social security numbers. Through exploitation of the DICOM protocol, installation of malicious code can be used to manipulate medical diagnosis, falsify scans, install malware, sabotage research, etc. Such threats could allow an attacker to compromise connected clinical devices and laterally spread malicious code to other parts of the network undetected.

Vulnerable Systems

The following systems/products are affected by these vulnerabilities per the Department of Homeland Security:

- Optima 520, which are medical imaging systems, all versions,
- Optima 540, which are medical imaging systems, all versions,
- Optima 640, which are medical imaging systems, all versions,
- Optima 680, which are medical imaging systems, all versions,
- Discovery NM530c, which is a nuclear medical imaging system, versions prior to Version 1.003,
- Discovery NM750b, which is a dedicated breast imaging system, versions prior to Version 2.003,

- Discovery XR656 and Discovery XR656 Plus, which are digital radiographic imaging systems, all versions,
- Revolution XQ/i, which is a medical imaging system, all versions,
- THUNIS-800+, which is a stationary diagnostic radiographic and fluoroscopic X-ray system, all versions,
- Centricity PACS Server, which is used to support a medical imaging archiving and communication system, all versions,
- Centricity PACS RA1000, which is used for diagnostic image analysis, all versions,
- Centricity PACS-IW, which is an integrated web-based system for medical imaging, all versions including Version 3.7.3.7 and Version 3.7.3.8,
- Centricity DMS, which is a data management software, all versions,
- Discovery VH / Millenium VG, which are nuclear medical imaging systems, all versions,
- eNTEGRA 2.0/2.5 Processing and Review Workstation, which is a nuclear medicine workstation for displaying, archiving, and communicating medical imaging, all versions,
- CADstream, which is a medical imaging software, all versions,
- Optima MR360, which is a medical imaging system, all versions,
- GEMNet License server (EchoServer), all versions,
- Image Vault 3.x medical imaging software, all versions
- Infinia / Infinia with Hawkeye 4 / 1, which are medical imaging systems, all versions,
- Millenium MG / Millenium NC / Millenium MyoSIGHT, which are nuclear medical imaging systems, all versions,
- Precision MP/i, which is a medical imaging system, all versions, and
- Xeleris 1.0 / 1.1 / 2.1 / 3.0 / 3.1, which are medical imaging workstations, all versions.

Patches, Mitigations & Workarounds:

The primary mechanism for protection against these vulnerabilities is to patch the impacted systems and ensure that patches are regularly applied. Due to the range of different patches available HC3 recommended that entities check their specific manufacture's website for detailed patch information.

Updated patches for specified PACS products are the best option as a patched vulnerability can no longer be exploited. HC3 also recommend the following mitigation actions:

- Implement a secure password on all PACS systems.
- Close all unused ports on affected systems.
- Enable encryption between the hosts in their PACS network using proper SSL certificates.
- Where possible, discontinue or limit the use of non-product-related third-party software, such as email and web browser software on the affected system.
- Ensure that affected systems have applied the most current vendor-issued patches available.
- Restrict network access to affected systems and ensure they are not directly accessible from the Internet.
- Implement network segmentation, and use DMZs with properly configured firewalls to selectively control, and monitor all traffic passed between zones and systems.
- Utilize full disk encryption capabilities to protect data on medical devices.
- When remote access is required, use secure methods such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

References

CVE-2012-6693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6693

CVE-2012-6694
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-6694

CVE-2013-7442
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-7442

CVE-2017-14008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14008

CVE-2018-17906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-17906

Millions of Medical Images Exposed, as US Fails to Secure PACS Flaws
https://healthitsecurity.com/news/millions-of-medical-images-exposed-as-us-fails-to-secure-pacs-flaws

DICOM file security: How malware can hide behind HIPAA-protected images
https://securityboulevard.com/2020/11/dicom-file-security-how-malware-can-hide-behind-hipaa-protected-images/

Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek.
https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

Confidential patient data freely accessible on the internet
https://www.greenbone.net/wp-content/uploads/CyberResilienceReport_EN.pdf

Billions of images left vulnerable online due to unsecured PACS
https://www.healthimaging.com/topics/imaging-informatics/billions-images-vulnerable-online-unsecured-pacs