LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Sector Alert

June 29, 2021 TLP: White Report: 202106291300

Picture Archiving Communication Systems (PACS) Vulnerabilities

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 demonstrated if the systems were exploited there could potentially be an issue with exposed patient data. These systems, which can be easily identified and compromised by hackers over the Internet, can provide unauthorized access and expose patient records. There continues to be several unpatched PACS servers visible and HC3 is recommending entities patch their systems immediately. Healthcare organizations are advised to review their inventory to determine if they are running any PACS systems and if so, ensure the guidance in this alert is followed.

Report

PACS was developed to assist the transition from analog to digital storage for medical images. PACS servers obtain images such as ultrasound, computed tomography (CT), magnetic resonance imaging (MRI) and radiography and stores them using the Digital Imaging and Communications in Medicine (DICOM) format. The use of the DICOM standard – which was developed three decades ago – is open to exploitation. In September 2019, researchers identified thousands of vulnerable PACS servers within the US health sector. A second study conducted several months later found the problem to be increasing, with additional systems identified as both vulnerable and accessible via the Internet. As of June 2021, these vulnerable systems are still widely deployed and available for exploitation. According to the most recent reporting, there are 130 health systems exposing about 8.5 million case studies, representing over 2 million patients, with approximately 275 million images related to their exams.

Vulnerable PACS servers face unnecessary exposure when directly connected to the Internet without applying basic security principles. PACS security begins by checking and validating connections to ensure access is limited only to authorized users. PACS systems should be configured in accordance with the documentation that accompanies them from their manufacturer. Internet connected systems should ensure traffic between them and physicians/patients is encrypted by enabling HTTPS. Furthermore, whenever possible they should be placed behind a firewall and a virtual private network (VPN) should be required to access them. The vulnerabilities associated with PACS systems 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. The following list of potentially vulnerable devices is not all-inclusive. The attack surface and overall security posture for all PACS systems should be reviewed, updated and maintained according to basic cybersecurity hygiene guidelines. These devices have known vulnerabilities according to the Department of Homeland Security:

- Optima 520, medical imaging systems, all versions
- Optima 540, medical imaging systems, all versions,
- Optima 640, medical imaging systems, all versions,
- Optima 680, medical imaging systems, all versions,
- Discovery NM530c, nuclear medical imaging system, versions prior to Version 1.003,
- Discovery NM750b, dedicated breast imaging system, versions prior to Version 2.003,
- Discovery XR656 and Discovery XR656 Plus, digital radiographic imaging systems, all versions,

- Revolution XQ/i, medical imaging system, all versions,
- THUNIS-800+, stationary diagnostic radiographic and fluoroscopic X-ray system, all versions,
- Centricity PACS Server, used to support a medical imaging archiving and communication system, all versions,
- Centricity PACS RA1000, used for diagnostic image analysis, all versions,
- Centricity PACS-IW, an integrated web-based system for medical imaging, all versions including Version 3.7.3.7 and Version 3.7.3.8,
- Centricity DMS, data management software, all versions,
- Discovery VH / Millenium VG, nuclear medical imaging systems, all versions,
- eNTEGRA 2.0/2.5 Processing and Review Workstation, nuclear medicine workstation for displaying, archiving, and communicating medical imaging, all versions,
- CADstream, medical imaging software, all versions,
- Optima MR360, 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, medical imaging systems, all versions,
- Millenium MG / Millenium NC / Millenium MyoSIGHT, nuclear medical imaging systems, all versions,
- Precision MP/i, medical imaging system, all versions, and
- Xeleris 1.0 / 1.1 / 2.1 / 3.0 / 3.1, medical imaging workstations, all versions.

References

Millions of medical images, patient data remain exposed via PACS flaws
https://www.scmagazine.com/featured/millions-of-medical-images-patient-data-remain-exposed-via-pacs-flaws/

HIPAA-Protected Malware? Exploiting DICOM Flaw to Embed Malware in CT/MRI Imagery
https://researchcylera.wpcomstaging.com/2019/04/16/pe-dicom-medical-malware/

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-pacsText

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback