CYBER SECURITY 2020-01

Cybersecurity proved to be a massive challenge for many in the healthcare sector in 2020 as providers worked to combat the COVID-19 crisis, while simultaneously being pummeled with targeted cyberattacks. These led to some of the biggest healthcare data breaches seen in recent years. (healthitsecurity.com)

All versions of iQ-WEB/VET-WEB 6.7.1 or lower have a vulnerability for cyber attacks

- Our cyber security specialists discovered a vulnerability in APACHE Server allowing remote attackers to gaining information even with no authentication. This vulnerability is caused by an Integer overflow. The CVSS (Common Vulnerability Scoring System) Score of this threat is 7.5 out of 10.
- Our cyber security specialists discovered some vulnerability such as SQL injection, XSS, CRF, … which cause increased Cyber-security threat and insufficient data security measures.

Increased cyber security of the application

Multiple security patches are applied in order to avoid system hacking. We strongly recommend all users of previous versions to upgrade their iQ-WEB to version 6.7.3, especially of those systems connected with the internet and those of large organizations.

INCREASE YOUR SECURITY AND REDUCE YOUR EXPOSURE TO CYBER SECURITY ATTACKS BY UPGRADING NOW!

Recent improvements (iQ-WEB 6.7.3)

- Up-to-date web server components (MySQL, Apache, PHP)
- Support of MySQL 5.7, Apache 2.4, PHP 7.2 .
- Enhanced email functionality (transmission via SSL/TLS protocol)
- Support for secure LDAP (SSL/TLS)
- HIPAA/GDPR compliant log information of shared WADO links (user, recipient, patient(s), studies, date/time) (NEW!)
- Dual authentication (suggested for email-based sharing of WADO links) (NEW!)
- Compliant with US and European data protection laws and regulations

How to communicate importance of upgrades?

- Attackers are constantly improving tactics and tools → older software applications may be vulnerable today.
- PACS contains highly sensitive personal information. Any leakage damages privacy.
- Hackers blackmail healthcare providers with sensitive data or demand money after privacy leakage.
- There is a high probability of severe financial damages to healthcare providers.
- It may be possible to prevent data loss after a hack using backups, but total cost of a full data retrieval may be enormous!

Why is updating Windows and/or Apache and/or Antivirus not sufficient?

- Only iQ-WEB 6.7.3 includes the updated MySQL, Apache and PHP files.
- In order to maintain the maximum level of security, all system components must be updated regularly.
- Being fully updated is also the only way to ensure legal compliance!

How likely is the risk and how serious are hacker incidents?

While this issue affects all users of PHP, fewer than one percent of IMAGE Information Systems' healthcare customers on all continents (both imaging centers and hospitals) were hacked in recent years. However, most hacker incidents will never be made public since healthcare providers fear losing public credibility, so the true rate of incidents is much higher than the public perception!
The main damage occurs when data is encrypted and held for ransom, resulting in a denial of service of radiology information systems and hospital information systems for days, and sometimes weeks.

All damages to iQ-SYSTEM PACS are easily avoided with our continuous cyber security upgrades.

Our Cyber Security experts are committed to keeping you safe.
Contact them via support@image-systems.biz if you have any questions or concerns!

UPDATE: THE 10 BIGGEST HEALTHCARE DATA BREACHES OF 2020

Much like in 2019, the biggest healthcare data breach of 2020 was caused by a third-party vendor, while ransomware and other risks dominated the threat landscape.

The healthcare sector saw a whopping 41.4 million patient records breached in 2019, fueled by a 49 percent increase in hacking, according to the Protenus Breach Barometer. And despite the COVID-19 crisis, the pace of healthcare data breaches in 2020 continue to highlight some of the sector's biggest vulnerabilities.

The end of 2019 saw a host of ransomware attacks and vendor-related breaches that outpaced previous years in the healthcare sector. For comparison, the industry saw just 15 million records breached in 2018.

-July 08, 2020 - Healthsecurity.com

BLACKBAUD: DOZENS OF HEALTHCARE ENTITIES, MILLIONS OF PATIENTS

Much like in 2019, the largest healthcare data breach was caused by a third-party vendor. The Blackbaud ransomware attack mirrored the AMCA breach, as it's still unclear just how much data and how many providers were affected.

It's estimated that more than two dozen providers and well over 10 million patients have been included in the final breach tally.

- July 07, 2020 - Healthsecurity.com

A ransomware attack on the Florida Orthopaedic Institute (FOI) potentially breached the data of about 640,000 patients, as reported to HHS on July 1.

The attack was first discovered on or about April 9, with the malware encrypting data stored on FOI servers. Administrators quickly secured the system, but the investigation revealed patient data was potentially exfiltrated or accessed during the attack.

The impacted data varied by patient, but could include a host of sensitive data such as Social Security numbers, dates of birth, claims addresses, insurance plan identification numbers, FOI claims histories, diagnosis codes, contact details, and physician locations, among other sensitive information.

- July 02, 2020 - Healthsecurity.com

IMAGE INFORMATION SYSTEMS EUROPE GMBH
LANGE STR. 16 | 18055 ROSTOCK | GERMANY
TEL. GER: +49 381 496 5820 | FAX GER: +49 381 496 582 99
TEL. US: +1 704 323 6663
WWW.IMAGE-SYSTEMS.BIZ | INFO@IMAGE-SYSTEMS.BIZ