CYBER SECURITY 2018-01

All versions of iQ-WEB/VET-WEB 6.4.5 or lower have a vulnerability for cyber attacks

- Our cyber security specialists discovered a vulnerability in PHP allowing remote attackers to cause a denial of service or possibly have unspecified greater impact. This vulnerability is caused by an Integer overflow. The CVSS (Common Vulnerability Scoring System) Score of this threat is 7.5 out of 10.
- The attacker needs very little knowledge or skill, and some system files on the server can be easily modified.
- **We recommend all customers to upgrade their iQ-WEB to version 6.6.2 immediately, especially those PACS systems connected to 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 6.6.2)

- Emails can be encrypted via SSL / TLS
- Update of web server components (PHP, MySQL etc.)

Scheduled improvements for 2018

- Two-factor authentication
- Update further components (eliminate old C++ redistributables)

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 6.6.2 includes the updated 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 2017. 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!

RECENT PUBLIC EXAMPLES OF ATTACKS

"Hospitals and GP surgeries in England and Scotland were among at least 16 health service organizations hit by a "ransomware" attack on Friday, using malware called Wanna Decryptor - with reports potentially dozens more were affected."
– May 2017 – Telegraph

"Dozens of hospital trusts across the country have been hit by a huge cyber attack, plunging the NHS into chaos. IT systems appear to have broken and emergency patients are being diverted to other areas, with hospitals across England and Scotland affected. The NHS was just one of the victims of the huge attack, which spread across the world infecting computers in 74 countries in Europe and Asia..."
– May 17, 2017 - Independent

"U.S. hospitals have been hit by the global ransomware attack...
Today, one of the largest drug makers in the U.S., Merck, reported being infected by the malware, as did the multinational law firm DLA Piper, which counts more than 20 offices in the U.S."
– June 27, 2017 – www.recode.net

"'Smart' Hospital IV Pump Vulnerable To Remote Hack Attack. The lack of security in the medical front is particularly alarming. The latest case in point: security researchers have discovered eight vulnerabilities in a syringe infusion pump used by hospitals to help administer medication to patients intravenously. The device is utilized to deliver medications, blood, antibiotics and other fluids to critical care patients, patients undergoing surgery (anesthesia) -- and newborn babies." – September 22, 2017
– www.techdirt.com

"GREENFIELD — Hancock Health paid a $55,000 ransom to hackers to regain access to its computer systems, hospital officials said. Part of the health network had been held hostage, when ransomware locked files including patient medical records. The hackers targeted more than 1,400 files, the names of every one temporarily changed to "I'm sorry." They gave the hospital seven days to pay or the files would be permanently encrypted, officials said."
– January 2018 – The Republic

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