DATA SECURITY UPDATE

Patching and Why It’s Important?

Unpatched software is one of the leading causes of data breaches for businesses.

Recent forensic investigation findings of account data compromises have shown that one of the key reasons for the loss of data is due to a lack of security patching. You may have heard of some security vulnerabilities like Spectre or Meltdown, however, there are many more that are sometimes only known to your service provider.

It’s thought that the vast majority of merchants are using out of date software, leaving them vulnerable to attack, as timely security updates aren’t being made. Criminals are preying on such users and are hacking their customers’ personal data, including card data. **By simply following your service provider’s instructions and installing the patches immediately, or as soon as possible, you can reduce your chance of becoming a victim.**

What’s a patch?

A patch is a piece of software designed to upgrade a computer programme to a more recent version. A patch can be required for a number of reasons, not only to introduce new features but also, and more importantly, to iron out any known security issues or vulnerabilities. These vulnerabilities, if not fixed, could mean your business is open to a cyberattack. These are sometimes known as critical patches.

Why’s patching important?

By not applying critical patches, the software installed on your website or elsewhere in your network becomes out of date. Criminals are able to exploit any known vulnerabilities associated with it. All it takes is for an attacker to identify that a patch hasn’t been installed to allow them the opportunity to access your web environment and lay the path to steal your customers’ data.

The Payment Card Industry Security Standards Council (PCI SSC) recently published an infographic and a short video to help educate merchants and businesses on the importance of patching.

Please click on the links below to view:

- PCI SSC Infographic: Patching
- PCI SSC Video: Patching

Service. Driven. Commerce

Global Payments is HSBC’s preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Service Regulations 2017 (504290) for the provision of payment services and under the Consumer Credit Act (714439) for the undertaking of terminal rental agreements. GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: Granite House, Granite Way, Syston, Leicester, LE7 1PL. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.

How and when are you notified about patches?

Like any software updates, patches are released by your service provider on a regular basis, dependent on the severity. It's up to you to ensure that you action all update requests as many will require your approval before they're actioned.

What about Approved Scanning Vendor (ASV) scans and how can they help?

ASV scans are a perimeter check of your website and/or your payment environment and form part of your Payment Card Industry Data Security Standards (PCI DSS) validation, dependant on your environment. ASV scans are looking for vulnerabilities or weaknesses that could be misused by someone to gain access to your systems and produce a report for any vulnerabilities identified. But what does this actually mean?

- It's a bit like having someone check your premises are physically secure - Have you locked the back door? Are your windows shut? Are there any known defects with your security alarm?
- The scans are basically highlighting that you may have left a port open, which hackers could gain entry through. Or, you're using an outdated and vulnerable piece of software and you are required to upgrade to the latest version/install a patch to fix the vulnerability.

Remember that an ASV scan shouldn't be used solely as a means to identify any vulnerabilities. It's up to you to ensure you install all critical security patches provided by your service provider!

PCI DSS patching requirements

It's worth noting that PCI DSS addresses the requirement to install security patches, **with critical patches required to be installed within one month of release, if not sooner**:

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.

Although applying patches or fixing vulnerabilities won't always prevent a breach, it'll definitely reduce the impact or the exposure to your business, which, in turn, will reduce any Card Scheme penalties under consideration!

Further useful resources from the PCI SSC:

- Defending Against Ransomware
- Defending Against Phishing & Social Engineering Attacks
- Protecting Your Customers' Payment Card Data from Malware
- Guide to Safe Payments Version 2.0 • August 2018