MAGENTO WEBSITE SECURITY REPORT

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN

TEL: +44 845 309 6232

JUNE 2020

PRODUCED BY FOREGENIX

OVERVIEW WHAT IS WEBSCAN?

We currently monitor over
200,000
Magento merchants
globally

WebScan is our comprehensive non-intrusive website scanning solution.
It analyses websites for specific security vulnerabilities to produce a risk score.

The scans are passive, meaning it looks for publicly available information (just like criminals do), and at no point does it try to exploit vulnerabilities.

WebScan looks for:

- Malware (including card skimmers)
- Platform and patching information
- SSL issues

We like to say that WebScan is the most up-to-date website scanning solution in the market as it is constantly updated by both our forensic team and Threat Intelligence Group.

CONTACT US

WWW.FOREGENIX.COM/WEBSCAN
TEL: +44 845 309 6232

JUNE 2020

OVERVIEW WHO IS FOREGENIX?

We are a leading independent cybersecurity company with a focus on keeping the world's payment systems secure.

With over a decade of experience in the **Payment Card Industry (PCI)**, we help merchants, payment processors, banks and other operators to ensure they are securing their environments effectively while complying with industry security standards.

We won the **Queen's Award for Enterprise** in 2019.

WHAT WE DO

COMPLIANCE & RISK

DIGITAL FORENSICS & RESPONSE

CYBERSECURITY TECHNOLOGY

FOREGENIX

JUNE 2020

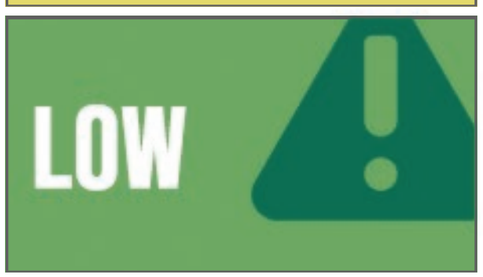
OVERVIEW WEBSCAN RISK SCORING DEFINITIONS

Already hacked, card data actively being stolen

At risk of being hacked - easily

THIS IS THE PROBLEM ZONE

Some issues, unlikely to get hacked



Hacking unlikely

FOREGENIX

JUNE 2020

OVERVIEW WEEKLY SUMMARY

More than **200,000 WEBSITES** remain on the Magento 1 platform

INCREASE of hacked Magento 2 websites since last month

95% of Magento 1 websites are High/Critical Risk

49% of Magento 2 websites are High/Critical Risk

MAGENTO IS STILL THE MOST TARGETED PLATFORM BY CRIMINALS

FOREGENIX

JUNE 2020

WEBSCAN RESULTS 6TH JULY 2020

Let's focus on Magento.

PLATFORM	MAY	JUNE	JULY
Magento 1	>200,000	-1.16%	-1.69%
Magento 2	>75,000	1.74%	3.51%

Magento 1 websites are slowly migrating off the platform, with a decrease of 1.69% over the last 30 days. Magento 2 websites are up 3.51% this month in comparison to June.

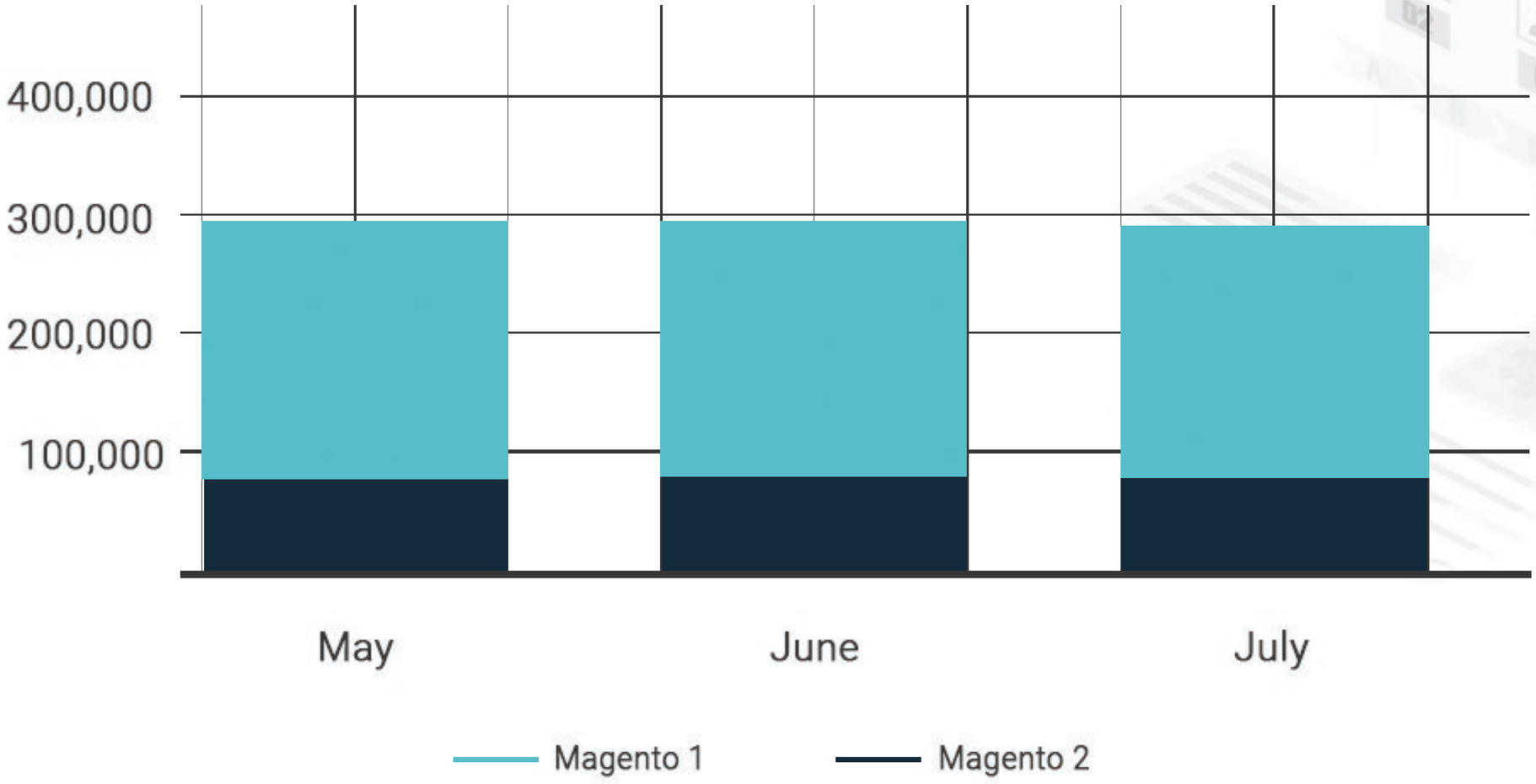
However, there are still more than 200,000 websites on the now unsupported Magento 1 platform.

The good news is that the number of hacked Magento 1 websites has decreased by 42 in the last 30 days from 2040 at the end of May. Unfortunately, hacked Magento 2 websites have increased by 47 to 418 at the end of June.

HIGH RISK	MAY	JUNE	JULY
Magento 1	207,925	206,021 ▼	201,267 ▼
Magento 2	37,703	39,993 ▲	39,415 ▼

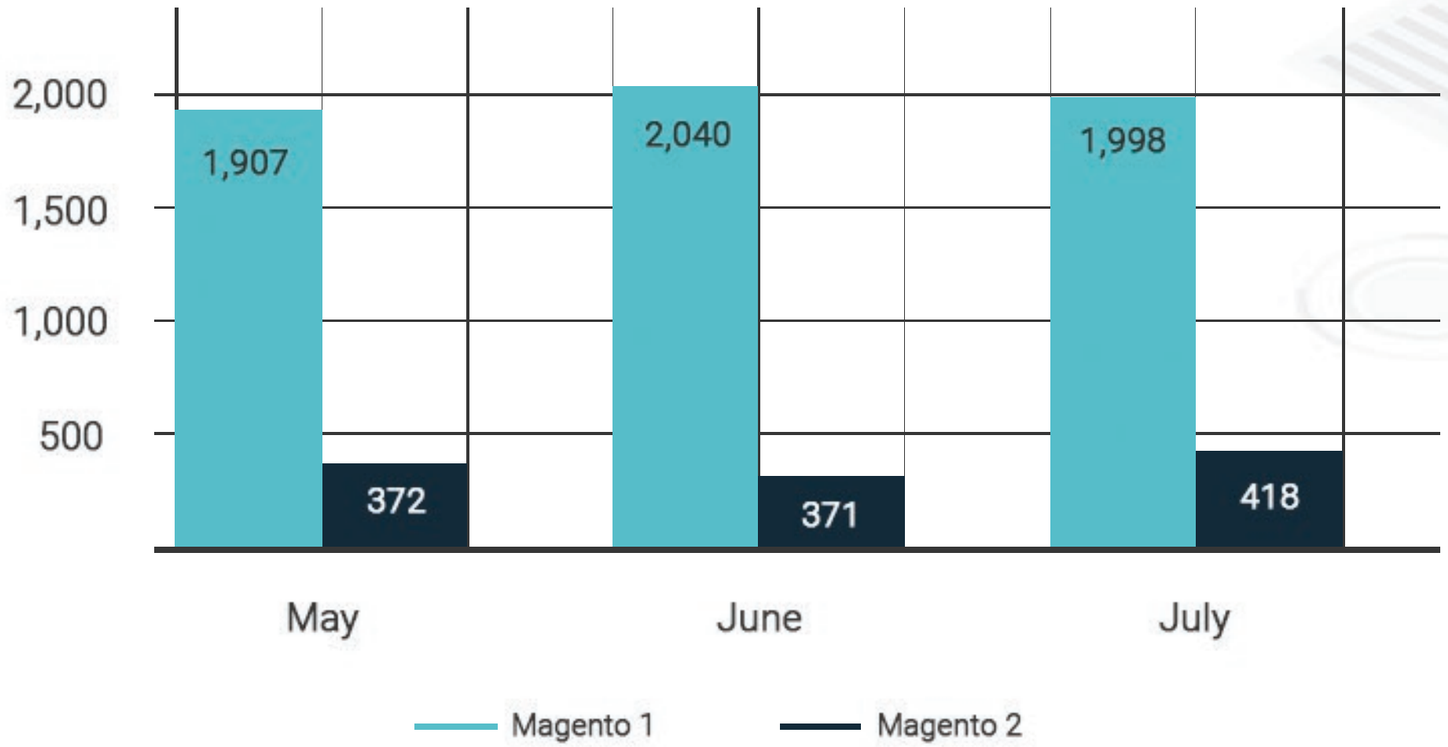
CRITICAL RISK	MAY	JUNE	JULY
Magento 1	1,907	2,040 ▲	1,998 ▼
Magento 2	372	371 ▼	418 ▲

WEBSCAN RESULTS WEBSITE NUMBERS (ALL MAGENTO)



WEBSCAN RESULTS CRITICAL RISK

Websites with Critical Risk have already been hacked (with card data being actively stolen). This month we have seen a **marginal increase** in the % of hacked websites on both Magento 1 and 2.

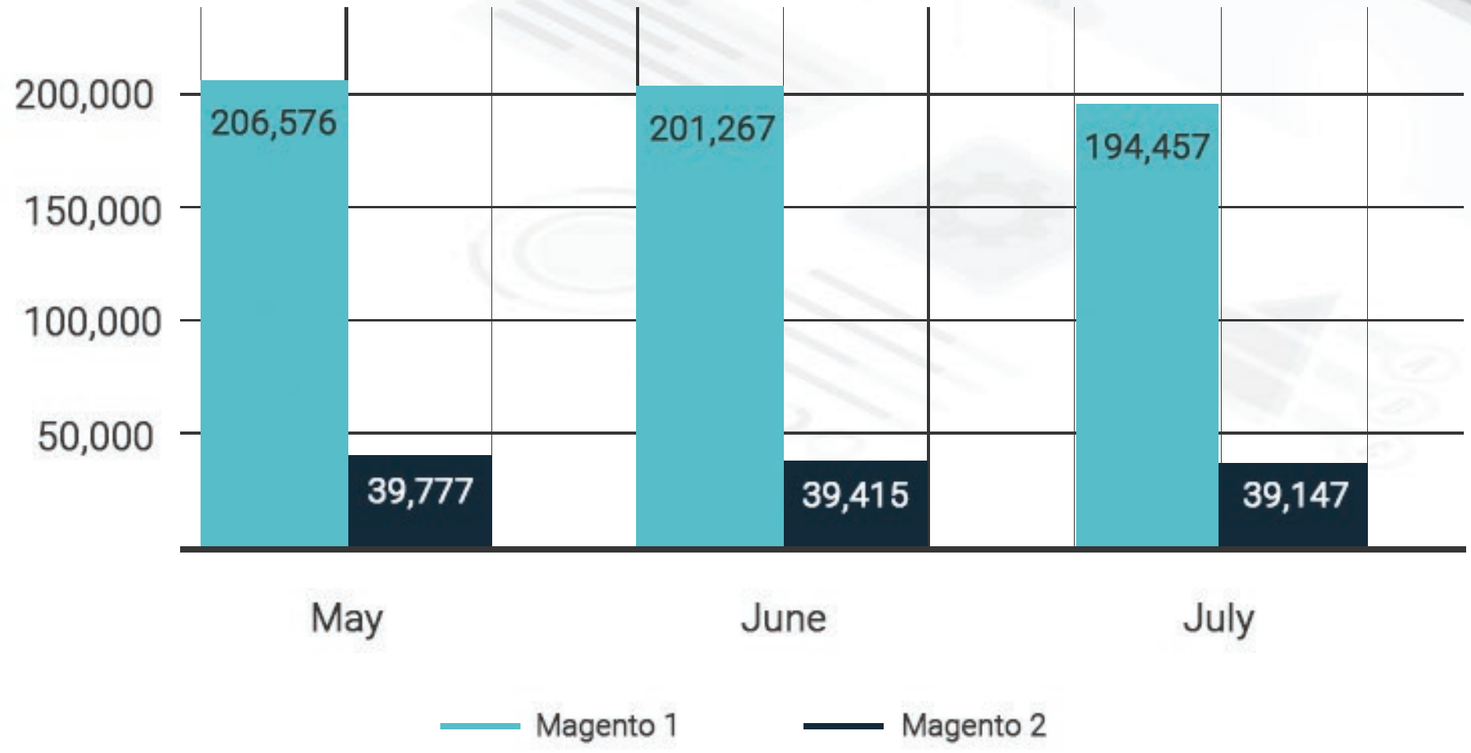


These websites have been individually verified by our Threat Intelligence Group as being hacked with card harvesting malware stealing customer payment data.

WEBSCAN RESULTS HIGH RISK

Websites with High Risk have significant security issues that make them very vulnerable to criminals. The sites have one or more of the following:

- Missing critical framework security patches
- Has known framework vulnerabilities
- Security issues with website set up
- Non Card Harvesting Malware



WEBSCAN RESULTS MALWARE DISTRIBUTION

Here's the Magento platform Malware breakdown:

MAGENTO 2

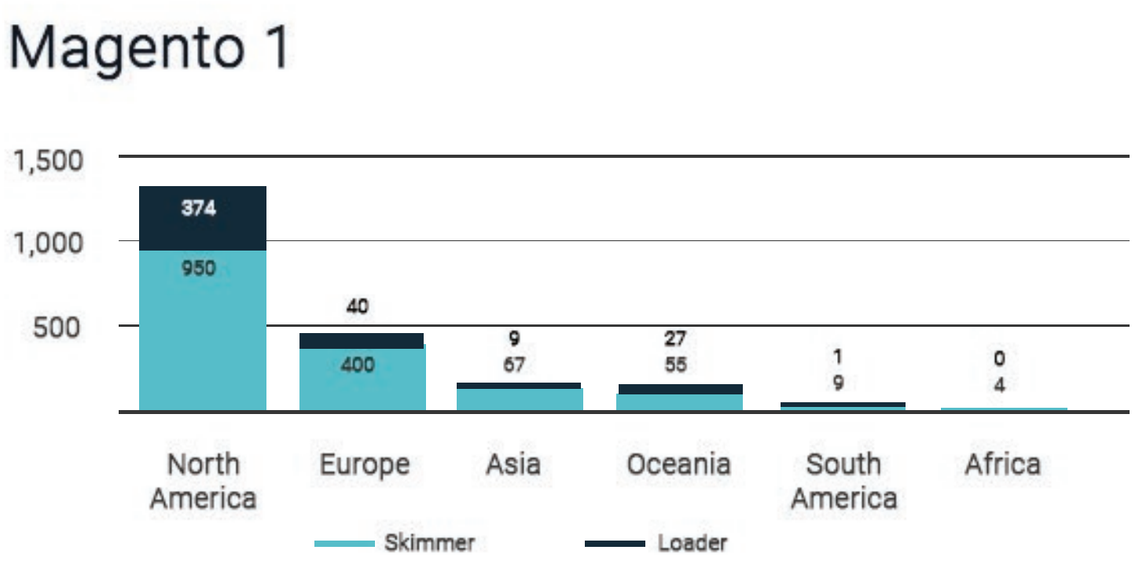
MAGENTO 1

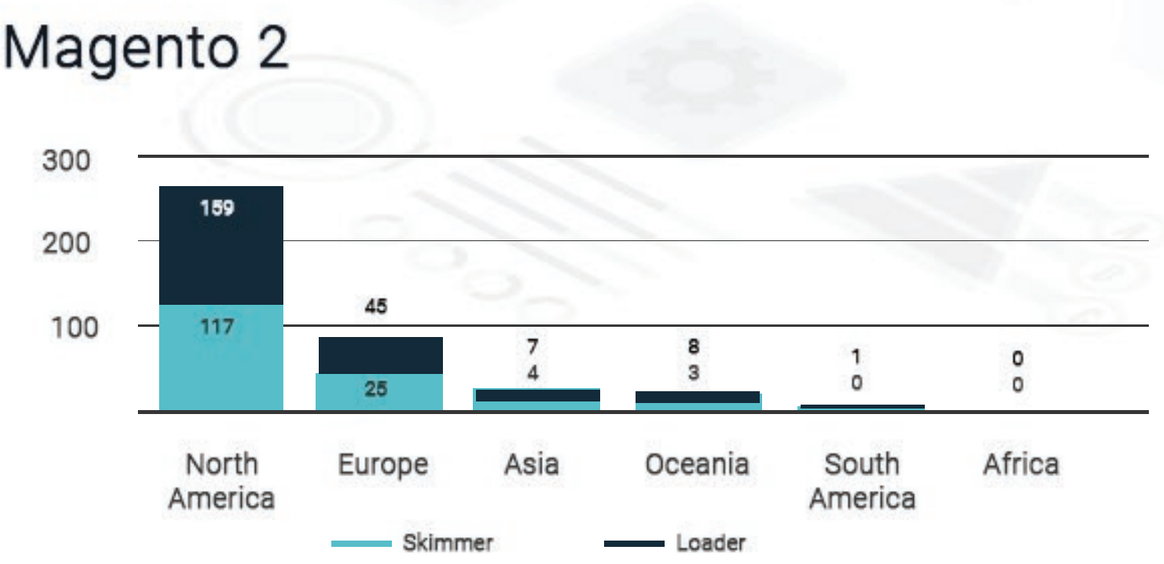
WEBSCAN RESULTS MAGENTO 1 & 2 - LOADERS & SKIMMERS

We also track how many websites are infected with loaders and skimmers.

Loaders are small pieces of code designed to load in additional malicious code onto a website.
Skimmers are malicious scripts designed to scrape card data and customer information from a site's payment page before sending them off to the attacker.

The charts below show which regions in the world have the highest infection rate.





FOREGENIX

JUNE 2020

WEBSCAN RESULTS MAGENTO 1 & 2 - FRAMEWORK ISSUES

Framework vulnerabilities are usually bugs in the software used to run your website.

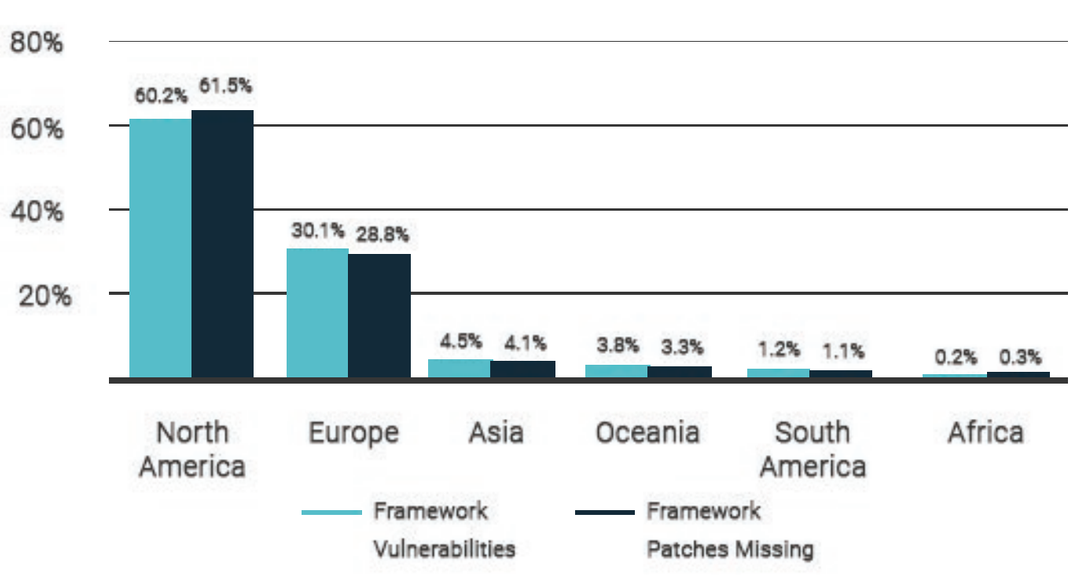
"**Framework security patches missing**" means your website is missing security patches/updates that are already available.

Framework issues also include insecure website set-up, such as leaving default settings in place (e.g. admin panel location, etc.).

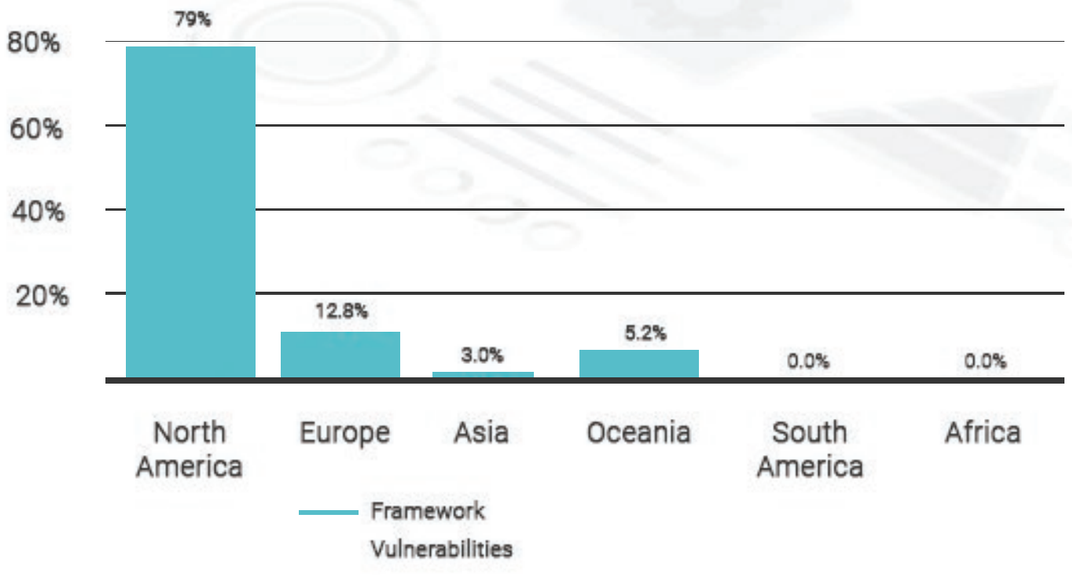
It's good to note that patching in Magento 2 works a bit differently than in Magento 1. With Magento 1, they released standalone security patches. This meant that websites could install these patches over older versions of Magento 1 and they would still be secure against the latest threats without having to update the entire site.

With Magento 2, they abandoned this practice and websites are expected to upgrade to the latest version of Magento if they want to stay secure.

Magento 1



Magento 2



FOREGENIX

JUNE 2020