TALA

REPORT

Unlimited Calls, Texts, Data (Sharing), Magecart?

Mobile providers in the EU gather a lot of highly-sensitive information from their customers. Are you getting more than you bargained for when you sign up online?

ALL THE USER EXPERIENCE, NONE OF THE SECURITY

Mobile service providers are no strangers to providing a content-rich user experience. But how good are they at securing it?

Few sectors collect as much sensitive information: from national ID/passport numbers and scans, to payslips, bank details and payment card information, the amount of data the average customer enters to sign up for a contract or buy services online is significant. What happens when the same applications and integrations that deliver that rich user experience inadvertently expose this sensitive information to leakage and theft?

We analyzed the websites of 13 of the top MSPs in 7 EU countries. This is what we found....

NONE of the sites had effective security in place:

With over 235 million customers between them, none of the mobile providers scored a passing grade for website security. Where a score of 80+ is considered reasonable and 50 is barely a passing grade, none of the mobile providers analyzed comes close:

Highest score was 33.5, with three sites returning a score of less than zero and none of the rest making it into double digits.

Average score: **4.5**

Copyright © Tala Security Inc, All Rights Reserved

100% of the sites are exposed to the most widespread website attack: cross-site scripting (XSS):

100% of the sites use dangerous JavaScript functions that could serve as injection points to initiate a DOM XSS attack.

Cross-site scripting is the most widespread website attack, resulting in significant sensitive data leakage.

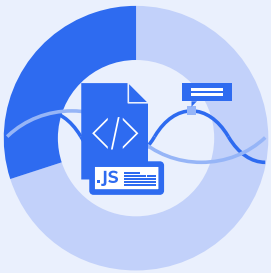
ALL of the sites have significant exposure to third-party JavaScript vulnerability:

735

The highest number of **3rd party JS on a single site**

162

Average number of **3rd party JS per site**



Both dynamic and static JavaScript distributions are double that found on the global Alexa 1000 websites**: almost 70% have dynamic and 35% static.**

SENSITIVE DATA IS AT SIGNIFICANT RISK: Form data exposure:

Each website uses forms to gather data, including passport numbers, bank details etc. but our analysis shows these connect to 20 domains - **25% more than the global Alexa 1000 average for websites** - this translates into excessive data sharing.

From a data privacy and security perspective, this number is massive:
To the casual observer, "form data" might not sound too serious but this is sensitive data, credentials, card transactions, passport scans, medical records...The kind of data you'd reasonably expect to be accessible to a website owner's servers and perhaps a payment clearing house - not unintentionally to multiple third-party integrations, owned and operated by vendors the customer knows nothing about, operating outside the security control of the website owner.

When website owners fail to secure data as it is entered into their websites, they're effectively leaving it hanging; the only reason it's not being stolen is that criminals haven't taken it. Yet.

Copyright © Tala Security Inc, All Rights Reserved

TALA

WHY IT MATTERS:

Unintentional data exposure is a significant, unaddressed problem for 100% of the EU mobile service providers analyzed.

Without controls, every piece of code running on websites - from every vendor included in the website owner's website supply chain - can modify, steal or leak information through client-side attacks enabled by JavaScript.

Every third party+ on a website represents a unique domain outside the security scope of the website owner.

In many cases, this data sharing is taking place via whitelisted, legitimate applications, without the website owner's knowledge: more than 99% of websites are at risk from trusted, whitelisted domains like Google Analytics. While these applications are set to collect data, many organizations aren't aware of exactly what kind of data they're collecting, or the extent of it. Even whitelisted apps can be exploited to exfiltrate data, with significant implications for data privacy, and by extension, GDPR. Unfortunately, the analysis here indicates that none of the EU telcos analysed here has sufficient awareness of the risk.

While most online businesses do a fine job of protecting data after the user has entered it, few seem to be aware of data leakage as an unintended consequence of the dynamic, rich website experience telcos are known for. This has potentially far-reaching consequences for GDPR - and for customers themselves - but no one seems to be talking about it.

If leaked, any combination of these would constitute an extremely serious breach for both the customer and the organization.

Copyright © Tala Security Inc, All Rights Reserved