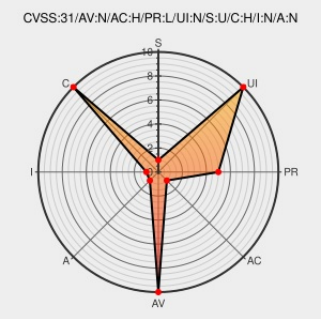
CVE-2017-3211

Published on: 01/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:31 PM UTC

CVE-2017-3211

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Yopify from Yopify contain the following vulnerability:

Yopify, an e-commerce notification plugin, up to April 06, 2017, leaks the first name, last initial, city, and recent purchase data of customers, all without user authorization.

CVE-2017-3211 has been assigned by cert@cert.org to track the vulnerability - currently rated as MEDIUM severity.

Yopify works by having the e-commerce site load a JavaScript widget from the Yopify servers, which contains both the code to generate the UI element and the data used to populate it, stored as JSON. This widget does not require any authorization beyond a site-specific API key, which is embedded in the e-commerce site's source code, and is easily extractable with a regular expression. The result is that by scraping a customer site to grab the API key and then simply running something like: curl 'https://yopify.com/api/yo/js/yo/3edb675e08e9c7fe22d243e44d184cdf/events.js?t=1490157080' where 3edb675e08e9c7fe22d243e44d184cdf is the site ID and t is a cache buster, someone can remotely grab the data pertaining to the last 50 customers. This is updated as purchases are made. Thus an attacker can poll every few hours for a few days/weeks/months and build up a database of an e-commerce site's customer set and associated purchasers. The data exposed to this polling was, however, far more extensive than the data displayed. While the pop-up only provides first name and last initial, the JSON blob originally contained first and last names in their entirety, along with city-level geolocation. While the casual online customer wouldn't have seen that, a malicious technical user could have trivially gained enough information to potentially target specific users of specific niche e-commerce sites.

Affected Vendor/Software: **Centire** - **Yopify** version **<= 2017-04-06**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	NONE	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
R7-2017-05 | CVE-2017-3211: Centire Yopify Information Disclosure	Exploit, Third Party Advisory, blog.rapid7.com, text/html	MISC blog.rapid7.com/2017/05/31/r7-2017-05-centire-yopify-information-disclosure-cve-2017-3211/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yopify	Yopify	All	All	All	All

cpe:2.3:a:yopify:yopify:*:*:*:*:*:*:*:*:

Discovery Credit

This vulnerability was discovered by Oliver Keyes, a Rapid7, Inc. senior data scientist.

← Previous ID

Next ID→