CESG REF: 54041238 / VULNERABILITY ID: 429485

CESG Vulnerability Report

February 2016

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

Summary

A vulnerability has been discovered in the NPAPI subsystem of Firefox which affects version 43.

This vulnerability has a Severity Score of 7.1 and a High Severity Rating (based on the Common Vulnerability Scoring System). The Severity Score and Severity Rating have been calculated from the Exploitability and Impact Metrics in Table 1.

Exploitability Metrics		Impact Metrics	
Metric	**Value**	**Metric**	**Value**
Access Vector	Network	Confidentiality Impact	None
Access Complexity	Medium	Integrity Impact	None
Authentication	None	Availability Impact	Complete

Table 1: Exploitability and Impact Metrics

Details

Firefox has suffered a regression of bug 445229. We believe there to be an incorrect assumption regarding the purpose of a certain variable assignment which is assumed to be obsolete. This may cause the NPAPI subsystem to crash.

This appears to affect Firefox versions after the following commit:
https://github.com/mozilla/gecko-Dev/commit /3163cfc2c163fb27251d1847898319300cedb51e

The code before this commit is as follows.

modules/plugin/base/src/nsJSNPRuntime.cpp

```
uint32_t generation = sNPObjWrappers.generation);

JSObject *obj = ::JS_NewObject(cx, &sNPObjectJSWrapperClass, nsnull,
nsnull);

if (generation != sNPObjWrappers.generation) {
    // Reload entry if the JS_NewObject call caused a GC and reallocated
    // the table (see bug 445229). This is guaranteed to succeed.

[0] entry = static_cast<NPObjWrapperHashEntry *>
        (PL_DHashTableOperate(&sNPObjWrappers, npobj, PL_DHASH_LOOKUP));
    NS_ASSERTION(entry && PL_DHASH_ENTRY_IS_BUSY(entry),
                 "Hashtable didn't find what we just added?");
}
```

The assignment at [0] is to re-validate a dangling pointer under certain conditions. The code after the commit is as follows.

dom/plugins/base/nsJSNRuntime.cpp

```
if (generation != sNPObjWrappers.Generation()) {
    // Reload entry if the JS_NewObject call caused a GC and reallocated
    // the table (see bug 445229). This is guaranteed to succeed.
```


This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

```
    NS_ASSERTION(PL_DHashTableSearch(&sNPObjWrappers, npobj),
                 "Hashtable didn't find what we just added?");
}
```

The comment, in both the before and after commits, explains the purpose of reloading the entry. There is an assumption that it is only required for the sake of the assertion. After changing the assertion to a format that does not require '`entry`', the re-assignment has been removed.

The removal of the assignment leads to a dangling pointer dereference in a non-standard feature of Firefox (the NPAPI plugin subsystem).

Proof of Concept

The high-level PoC to trigger the vulnerability and cause a crash is as follows:

1. write a NPAPI plug-in which has a function that creates and returns a new NPObject every time it is called;
2. call that function in a loop from Javascript.

The browser will likely crash when a HashTable Object resizes its underlying data storage.

Contact Information

The CESG mailbox for vulnerability disclosure is 'security@cesg.gsi.gov.uk'. Please contact us for our PGP key.

Crediting CESG

CESG would appreciate appropriate credit in any advisories which you may publish about this issue.

Verification, Resolution and Release

Please inform CESG via the 'security@cesg.gsi.gov.uk' mailbox, quoting the CESG Reference above, should you:

- confirm that this is a security issue;
- allocate the issue a CVE identifier;
- determine a date to release a patch;
- determine a date to publish advisories.

CESG Disclosure Policy

CESG has adopted the ISO 29147 approach to vulnerability disclosure, and as-such follows a co-ordinated disclosure approach with affected parties. We have never publicly disclosed a vulnerability prior to a fix being made available.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

CESG recognises that vendors need a reasonable amount of time to mitigate a vulnerability, for example, to understand the impact to customers, to triage against other vulnerabilities, to implement a fix in coordination with others, and to make that fix available to its customers. As this will vary based on the exact situation CESG does not define a set time frame in which a fix must be made available, and we are happy to discuss the circumstances of any particular disclosure.

If CESG believes a vendor is not making appropriate progress with vulnerability resolution, we may, after discussion with the vendor, choose to share the details appropriately (for example, with service providers and our customers) to ensure that we provide appropriate mitigation of the threat to the UK and to UK interests.

Terms of Reference

Please note, any CESG findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

(c) Crown Copyright 2016. CESG shall at all times retain Crown copyright in this document and the permission of CESG must be sought in advance if you want to copy, republish, translate or otherwise reproduce all or any part of the document, or disclose or release all or any part of it to another person.

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk