



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

November 3, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:

SA2015-127

DATE(S) ISSUED:

11/03/2015

SUBJECT:

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been identified in Mozilla Firefox, which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 42
- Mozilla Firefox ESR versions prior to 38.4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Mozilla has confirmed multiple vulnerabilities in Firefox, Firefox ESR, and Firefox OS. Exploitation of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user or vulnerable application, crash the affected application, disclose sensitive information, bypass the same-origin policy and other security restrictions, and perform unauthorized actions. These vulnerabilities could be exploited if a user visits or is redirected to a specially-crafted webpage or opens a specially-crafted file. Details of these vulnerabilities are as follows:

- A buffer-overflow vulnerability because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'TextureStorage11' module of the 'ANGLE' graphics library. (CVE-2015-7198)
- A memory-corruption vulnerability occurs due to use-after-poison error. Specifically, this issue affects the 'sec_asn1d_parse_leaf()' function of ASN.1 decoder. (CVE-2015-7181)
- A heap-based buffer-overflow vulnerability because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue occurs when parsing octet string. (CVE-2015-7182)
- A memory-corruption vulnerability occurs due to a buffer underflow error. Specifically, this issue affects the 'libjar' library. An attacker can exploit this issue through a specially crafted ZIP file. (CVE-2015-7194)
- Multiple security-bypass vulnerabilities because it fails to properly perform proper status check in SVG rendering process and cryptographic key manipulation. Specifically, these issues affect the 'AddWeightedPathSegLists' and 'SVGPathSegListSMILType::Interpolate' modules. (CVE-2015-7199, CVE-2015-7200)
- A denial-of-service vulnerability occurs due to an error in interaction between 'Java applets' and 'JavaScript'. Specifically, this issue occurs because the Java plugin deallocates a JavaScript wrapper when it is still in use. This issue is specific to systems where Java is installed and enabled as a browser plugin. (CVE-2015-7196)
- A same-origin security-bypass vulnerability occurs due to an error in processing multiple media types in 'Content-Type' headers from a server. An attacker can exploit this issue to bypass Cross-origin resource sharing (CORS) and 'preflight' with simple requests against the CORS specification. (CVE-2015-7193)
- A heap-based buffer-overflow vulnerability because it fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Specifically, this issue affects the 'nsJPEGEncoder()' function. This issue occurs during script interactions with a 'canvas' element. (CVE-2015-7189)
- Multiple security-bypass vulnerabilities occurs due to memory-safety errors. Specifically, this issue occurs in the browser engine. An attacker can exploit these issues to execute arbitrary code or cause denial-of-service condition. (CVE-2015-7188)
- Multiple security-bypass vulnerabilities occurs due to memory-safety errors. Specifically, these issues occurs in the browser engine. An attacker can exploit these issues to execute arbitrary code or cause denial-of-service condition. (CVE-2015-4513, CVE-2015-4514)
- A security-bypass vulnerability. Specifically, this issue occurs because it is possible to bypass secure requirements for 'WebSockets' when web workers are used to create WebSockets. (CVE-2015-7197)

- An information-disclosure vulnerability. Specifically, the issue occurs because 'Workstation' field is populated with the hostname of the system making the request. An attacker can exploit this issue by sending a specially crafted web page to disclose the hostname and windows domain through NTLM-based HTTP authentication. (CVE-2015-4515)
- A security-bypass vulnerability because Reader View disables script for rendered pages through a whitelist of allowed HTML content. An attacker can exploit this issue by sending a specially crafted web page to bypass content security policy (CSP) protections and may allow cross-site scripting attacks. (CVE-2015-4518)
- A security-bypass vulnerability because it fails to restore the address bar after exiting the fullscreen mode. An attacker can exploit this issue to spoof the address bar. (CVE-2015-7185)
- A security-bypass vulnerability because it allows a locally saved HTML file to use 'file:>/code>' URIs. An attacker can exploit this issue to bypass same-origin policy and trigger the download of additional files or open cached profile data. (CVE-2015-7186)
- A security-bypass vulnerability because it allows to execute an inline script of the extension even when it is disabled. An attacker can exploit this issue to execute an arbitrary extension. (CVE-2015-7187)
- A privilege-escalation vulnerability because it execute an URL with system privileges when crash reporter is used. Specifically, this issue occurs when it is launched through an Android intent. An attacker can exploit this issue to read local log files, access private information and load local HTML files through 'file:' URIs. This issue affects Android versions 4.4 and earlier only. (CVE-2015-7190)
- A cross-site scripting vulnerability because it fails to properly sterilize opened addresses sent to Firefox through intents. An attacker can exploit this issue through Android intents and fallback navigation. (CVE-2015-7191)
- A denial-of-service vulnerability occurs when an accessibility tool requests the index of a table row through the 'NSAccessibilityIndexAttribute' value. Specifically, this issue affects the accessibility tools on OS X. An attacker can exploit this issue to crash the application. This issue is specific to Mac OS X systems only. (CVE-2015-7192)
- A security-bypass vulnerability because it fails to properly parse URLs with certain escaped characters in hostnames. An attacker can exploit this issue to potential extraction of site specific tokens. (CVE-2015-7195)

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Mozilla:

<https://www.mozilla.org/en-US/security/advisories/mfsa2015-116>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-117>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-118>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-119>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-120>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-121>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-122>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-123>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-124>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-125>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-126>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-127>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-128>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-129>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-130>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-131>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-132>
<https://www.mozilla.org/en-US/security/advisories/mfsa2015-133>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4513>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4514>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4515>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4518>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7185>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7186>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7187>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7188>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7189>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7190>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7191>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7192>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7193>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7194>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7195>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7196>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7197>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7198>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7199>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7200>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7181>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7182>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7183>

expiration time (CVE-2015-6999).

- An input validation issue existed in the kernel. This issue was addressed through improved input validation (CVE-2015-7004).
- An issue existed in the authorization checks for querying phone call status. This issue was addressed through additional authorization state queries (CVE-2015-7022).
- An issue existed when reusing virtual memory. This issue was addressed through improved validation (CVE-2015-6994).
- An uninitialized memory issue existed in the kernel. This issue was addressed through improved memory initialization (CVE-2015-6988).

- Multiple memory corruption issues existed in CoreGraphics. These issues were addressed through improved memory handling (CVE-2015-5925, CVE-2015-5926).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5927, CVE-2015-5942, CVE-2015-6976, CVE-2015-6977, CVE-2015-6978, CVE-2015-6990, CVE-2015-6991, CVE-2015-6993, CVE-2015-7008, CVE-2015-7009, CVE-2015-7010, CVE-2015-7018).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6975, CVE-2015-6992, CVE-2015-7017).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5935, CVE-2015-5936, CVE-2015-5937, CVE-2015-5939).
- Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling (CVE-2015-5928, CVE-2015-5929, CVE-2015-5930, CVE-2015-6981, CVE-2015-6982, CVE-2015-7002, CVE-2015-7005, CVE-2015-7012, CVE-2015-7014).
- The kSecRevocationRequirePositiveResponse flag was specified but not implemented. This issue was addressed by implementing the flag (CVE-2015-6997).
- When "Show on Lock Screen" was turned off for Phone or Messages, configuration changes were not immediately applied. This issue was addressed through improved state management (CVE-2015-7000).
- A double free issue existed in the handling of AtomicBufferedFile descriptors. This issue was addressed through improved validation of AtomicBufferedFile descriptors (CVE-2015-6983).
- A file traversal vulnerability existed in the handling of CPIO archives. This issue was addressed through improved validation of metadata (CVE-2015-7006).
- A heap based buffer overflow issue existed in the DNS client library. A malicious application with the ability to spoof responses from the local configd service may have been able to cause arbitrary code execution in DNS clients (CVE-2015-7015).
- A memory corruption issue existed in ATS. This issue was addressed through improved memory handling (CVE-2015-6985).
- A memory corruption issue existed in IOAcceleratorFamily. This issue was addressed through improved memory handling (CVE-2015-6996).
- A memory corruption issue existed in OpenGL. This issue was addressed through improved memory handling (CVE-2015-5924).
- A memory corruption issue existed in the Accelerate Framework in multi-threading mode. This issue was addressed through improved accessor element validation and improved object locking (CVE-2015-5940).
- A memory corruption issue existed in the handling of dispatch calls. This issue was addressed through improved memory handling (CVE-2015-6989).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-6974).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-7021).
- A memory corruption issue existed in the parsing of disk images. This issue was addressed through improved memory handling (CVE-2015-6995).

- A method existed for applications to create synthetic clicks on keychain prompts. This was addressed by disabling synthetic clicks for keychain access windows (CVE-2015-5943).
- A parsing issue existed when handling cookies with different letter casing. This issue was addressed through improved parsing (CVE-2015-7023).
- A privilege separation issue existed in PAM support. This issue was addressed with improved authorization checks (CVE-2015-6563).
- A type confusion issue existed in the validation of Mach tasks. This issue was addressed through improved Mach task validation (CVE-2015-5932).
- An entitlement validation issue existed in Managed Configuration. A developer-signed app could bypass restrictions on use of restricted entitlements and elevate privileges. This issue was addressed through improved provisioning profile validation (CVE-2015-7016).
- An input validation issue existed in parsing bookmark metadata. This issue was addressed through improved validation checks (CVE-2015-6987).
- An input validation issue existed when handling NVRAM parameters. This issue was addressed through improved validation (CVE-2015-5945).
- An issue existed when reusing virtual memory. This issue was addressed through improved validation (CVE-2015-6994).
- An issue existed with EFI argument handling. This was addressed by removing the affected functions (CVE-2015-7035).
- An issue existed within the path validation logic for symlinks. This issue was addressed through improved path sanitization (CVE-2015-6984).
- An uninitialized memory issue existed in coreaudiod. This issue was addressed through improved memory initialization (CVE-2015-7003).
- An uninitialized memory issue existed in the kernel. This issue was addressed through improved memory initialization (CVE-2015-6988).
- In some circumstances, Script Editor did not ask for user confirmation before executing AppleScripts. This issue was addressed by prompting for user confirmation before executing AppleScripts (CVE-2015-7007).
- Multiple issues existed in netsh version 5.6. These issues were addressed by using patches affecting OS X from upstream (CVE-2012-6151, CVE-2014-3565).
- Multiple memory corruption issues existed in CoreGraphics. These issues were addressed through improved memory handling (CVE-2015-5925, CVE-2015-5926).
- Multiple memory corruption issues existed in the handling of audio files. These issues were addressed through improved memory handling (CVE-2015-5933, CVE-2015-5934).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5927, CVE-2015-5942, CVE-2015-6976, CVE-2015-6977, CVE-2015-6978, CVE-2015-6991, CVE-2015-6993, CVE-2015-7009, CVE-2015-7010, CVE-2015-7018).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5944).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6975).

- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6990, CVE-2015-7008).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6992).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-7017).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5935, CVE-2015-5938).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5936, CVE-2015-5937, CVE-2015-5939).
- Multiple out of bounds read issues existed in the NVIDIA graphics driver. These issues were addressed through improved bounds checking (CVE-2015-7019, CVE-2015-7020).
- Multiple vulnerabilities existed in PHP versions prior to 5.5.29 and 5.4.45. These were addressed by updating PHP to versions 5.5.29 and 5.4.45 (CVE-2015-0235, CVE-2015-0273, CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838).

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and bypassing security restrictions. Failed attacks may still cause a Denial of Service condition within the targeted delivery method. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:

<https://support.apple.com/en-us/ht201222>

CVE

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0273>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3565>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5916>

