



CVE-2015-7178

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-7178
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-24 04:59:00 UTC
Updated	2016-12-22 03:00:00 UTC
Description	The ProgramBinary::linkAttributes function in libGLES in ANGLE, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.0.5, does not properly validate the length of the linkAttributes string, which allows attackers to trigger a buffer overflow and execute arbitrary code on the target system.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	38.0.1	All	All	All
Application	Mozilla	Firefox Esr	38.0.5	All	All	All
Application	Mozilla	Firefox Esr	38.1.0	All	All	All
Application	Mozilla	Firefox Esr	38.1.1	All	All	All
Application	Mozilla	Firefox Esr	38.2.0	All	All	All
Application	Mozilla	Firefox Esr	38.2.1	All	All	All

References
Reference
Oracle Solaris Bulletin - April 2016
[security-announce] openSUSE-SU-2015:1681-1: important: Security update
[security-announce] openSUSE-SU-2015:1658-1: important: Security update
1189860 - (CVE-2015-7178) Missing bounds check causes memory-safety bug in ProgramBinary::linkAttributes
[security-announce] openSUSE-SU-2015:1679-1: important: Security update
Mozilla Firefox Multiple Security Vulnerabilities
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction
Memory safety errors in libGLES in the ANGLE graphics library — Mozilla
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.