



CVE-2013-0780

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2013-0780
State	PUBLISHED
Assigner	mozilla
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-19 23:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Use-after-free vulnerability in the nsOverflowContinuationTracker::Finish function in Mozilla Firefox before 19.0, Firefox ESF

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-416 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
USN-1729-1: Firefox vulnerabilities Ubuntu			af854a3a-2127-422b-91ae-3	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-3	
USN-1729-2: Firefox regression Ubuntu			af854a3a-2127-422b-91ae-3	
Red Hat Customer Portal			af854a3a-2127-422b-91ae-3	
USN-1748-1: Thunderbird vulnerabilities Ubuntu			af854a3a-2127-422b-91ae-3	
openSUSE-SU-2013:0324-1: moderate: Mozilla Februarys			af854a3a-2127-422b-91ae-3	
MFSA 2013-28: Use-after-free, out of bounds read, and buffer overflow issues found using Address Sanitizer			af854a3a-2127-422b-91ae-3	
[security-announce] openSUSE-SU-2013:0323-1: important: Mozilla: Februar			af854a3a-2127-422b-91ae-3	
Debian -- Security Information -- DSA-2699-1 iceweasel			af854a3a-2127-422b-91ae-3	
812893 – (CVE-2013-0780) Heap-use-after-free in nsOverflowContinuationTracker::Finish, with -moz-columns			af854a3a-2127-422b-91ae-3	
Repository / Oval Repository			af854a3a-2127-422b-91ae-3	
CVE Program record			CVE.ORG	
NVD vulnerability detail			NVD	
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				