



CVE-2015-3335

Published on: 04/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

CVE-2015-3335

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

The `NaClSandbox::InitializeLayerTwoSandbox` function in `components/nacl/loader/sandbox_linux/nacl_sandbox_linux.cc` in Google Chrome before 42.0.2311.90 does not have `RLIMIT_AS` and `RLIMIT_DATA` limits for Native Client (aka NaCl) processes, which might make it easier for remote attackers to conduct row-hammer

attacks or have unspecified other impact by leveraging the ability to run a crafted program in the NaCl sandbox.

CVE-2015-3335 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Google Chrome 'nacl_sandbox_linux.cc'
Remote Security Vulnerability

[Third Party Advisory](#)
[VDB Entry](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 72715](#)

openSUSE-SU-2015:0748-1: moderate:
Security update for Chromium

[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[🐉 SUSE openSUSE-SU-2015:0748](#)

Chrome Releases: Stable Channel Update

[Release Notes](#)
[Vendor Advisory](#)
[googlechromereleases.blogspot.com](#)

[🌐 CONFIRM](#)
[googlechromereleases.blogspot.com/2015/04/stable-channel-update_14.html](#)

text/html

455839 - chromium - An open-source project to help move the web forward. - Monorail

Exploit

Vendor Advisory

code.google.com

text/html

CONFIRM

code.google.com/p/chromium/issues/detail?id=455839

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
cpe:2.3:a:google:chrome:*****:						
cpe:2.3:o:opensuse:opensuse:13.1:*****:						
cpe:2.3:o:opensuse:opensuse:13.2:*****:						
cpe:2.3:o:opensuse:opensuse:13.1:*****:						
cpe:2.3:o:opensuse:opensuse:13.2:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)