

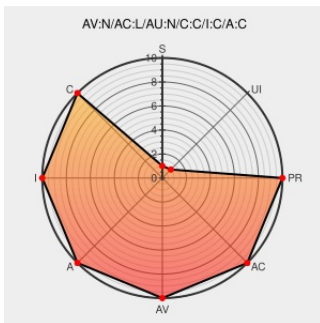


CVE-2014-3188

Published on: 10/08/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-3188

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

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

Google Chrome before 38.0.2125.101 and Chrome OS before 38.0.2125.101 do not properly handle the interaction of IPC and Google V8, which allows remote attackers to execute arbitrary code via vectors involving JSON data, related to improper parsing of an escaped index by ParseJsonObject in json-parser.h.

CVE-2014-3188 has been assigned by security@google.com to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Red Hat Customer Portal

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2014:1626](#)

v8 - V8 JavaScript Engine - Monorail

[code.google.com](#)
[text/html](#)

[CONFIRM code.google.com/p/v8/source/detail?r=24125](#)

Chrome Releases: Stable Channel Update

[Vendor Advisory](#)
[googlechromereleases.blogspot.com](#)
[text/html](#)

[CONFIRM googlechromereleases.blogspot.com/2014/10/stable-channel-update.html](#)

Chrome Releases: Stable Channel Update for Chrome OS

[Vendor Advisory](#)
[googlechromereleases.blogspot.com](#)
[text/html](#)

[CONFIRM googlechromereleases.blogspot.com/2014/10/stable-channel-update-for-chrome-os.html](#)

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	Google	Chrome Os	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary Eus	6.6.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary Eus	6.6.z	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All

```
cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:google:chrome_os:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:6.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:6.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server supplementary:6.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise_linux_server_supplementary:6.0:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_server_supplementary_eus:6.6.z:*.*:*.*:*.:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_supplementary_eus:6.6.z:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux workstation supplementary:6.0:*.***.***.*
```

cpe:2.3:o:redhat:enterprise_linux_workstation_supplementary:6.0:*:*:*:*:*:

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](#)