



CVE-2016-7153

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

Summary

CVE	CVE-2016-7153
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-06 10:59:00 UTC
Updated	2017-02-19 06:22:00 UTC
Description	The HTTP/2 protocol does not consider the role of the TCP congestion window in providing information about content length

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Google	Chrome	-	All	All	All
Application	Google	Chrome	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Edge	-	All	All	All
Application	Microsoft	Internet Explorer	-	All	All	All
Application	Microsoft	Internet Explorer	-	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Opera	Opera Browser	-	All	All	All
Application	Opera	Opera Browser	-	All	All	All

References

Reference

Microsoft Internet Explorer HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information | Ars Technica

New attack steals SSNs, e-mail addresses, and more from HTTPS pages | Ars Technica

Apple Safari HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information on the
tom.vg/papers/heist_blackhat2016.pdf

HTTP/2 CVE-2016-7153 Information Disclosure Vulnerability

Mozilla Firefox HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information on t

Opera HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information on the Target

Google Chrome HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information fro

Microsoft Edge HTTPS API Attack Against TCP Congestion Window Protocol Lets Remote Users Obtain Potentially Sensitive Information on t

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.

© [CVE.report](#) 2026 |

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](#)