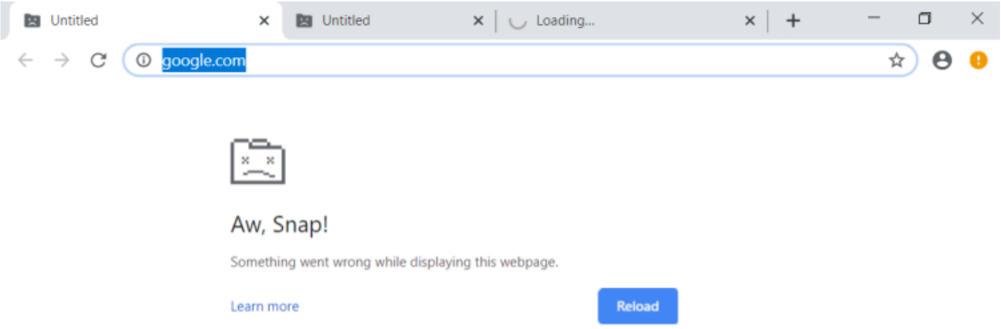
text/plain

ericlaw talks about the web and software in general

Aw, snap! What if Every Tab Crashes?

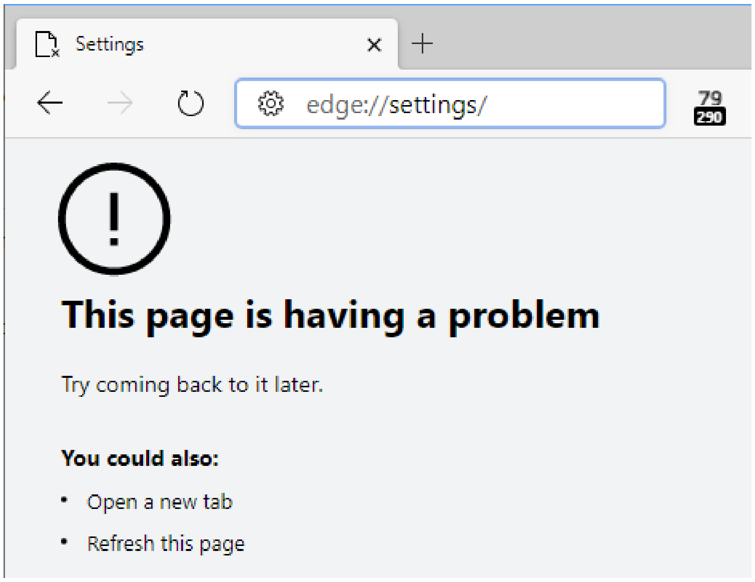
For a small number of users of Chromium-based browsers (including Chrome and the new Microsoft Edge) on Windows 10, after updating to 78.0.3875.0, every new tab crashes immediately when the browser starts.

Impacted users can open as many new tabs as they like, but each will instantly crash:



Aw, Snap!

Something went wrong while displaying this webpage.



This page is having a problem

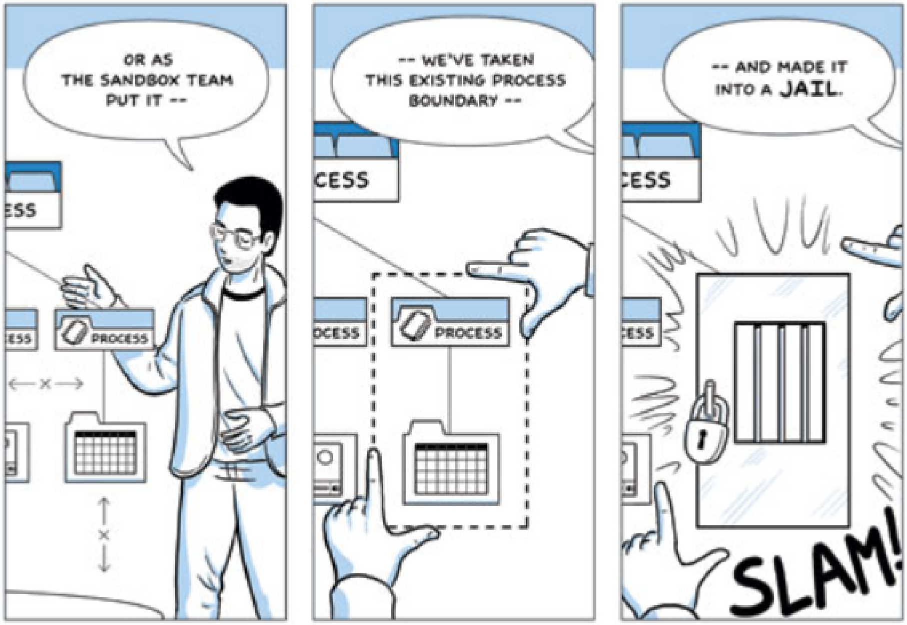
Try coming back to it later.

You could also:

As of **Chrome 81.0.3992**, the page will show the string **Error Code: STATUS_INVALID_IMAGE_HASH**.

What's going wrong?

This problem relates to a security/reliability improvement made to **Chromium's sandboxing**. Chromium runs each of the tabs (and extensions) within locked down ("sandboxed") processes:


OR AS THE SANDBOX TEAM PUT IT --
ESS
ESS
PROCESS
-- WE'VE TAKEN THIS EXISTING PROCESS BOUNDARY --
CESS
OCESS
PROCESS
-- AND MADE IT INTO A JAIL.
CESS
ESS
SLAM!

In Chrome 78, a change was made to prevent 3rd-party code from injecting itself into these sandboxed processes. 3rd-party code is a top source of browser reliability and performance problems, and it has been a longstanding goal for browser vendors to get this code out of the web platform engine.

This new feature relies on setting a **Windows 10** **Process Mitigation policy** that instructs the OS loader to refuse to load binaries that aren't signed by Microsoft. **Edge 13** enabled this mitigation in 2015, and the Chromium change brings parity to the new Edge 78+. Notably, Chrome's own DLLs aren't signed by Microsoft so they are **specially exempted** by the Chromium sandboxing code.

Unfortunately, the impact of this change is that the renderer is killed (**resulting in the "Aw snap" page**) if any disallowed DLL attempts to load, for instance, if your antivirus software attempts to inject its DLLs into the renderer processes. For example, Symantec Endpoint Protection versions **before 14.2** are **known** to trigger this problem.

If you encounter this problem, you should follow the following steps:

Update any security software you have to the latest version.

Other than malware, security software is the other likely cause of code being unexpectedly injected into the renderers.

Temporarily disable the new protection

You can temporarily launch the browser without this sandbox feature to verify that it's the source of the crashes.

1. Close all browser instances (verify that there are no hidden chrome.exe or msedge.exe processes using Task Manager)
2. Use Windows+R to launch the browser with the command line override:

```
msedge.exe --disable-features=RendererCodeIntegrity
```

or

```
chrome.exe --disable-features=RendererCodeIntegrity
```

Ensure that the tab processes work properly when code integrity checks are disabled.

If so, you’ve proven that code integrity checks are causing the crashes.

Hunt down the culprit

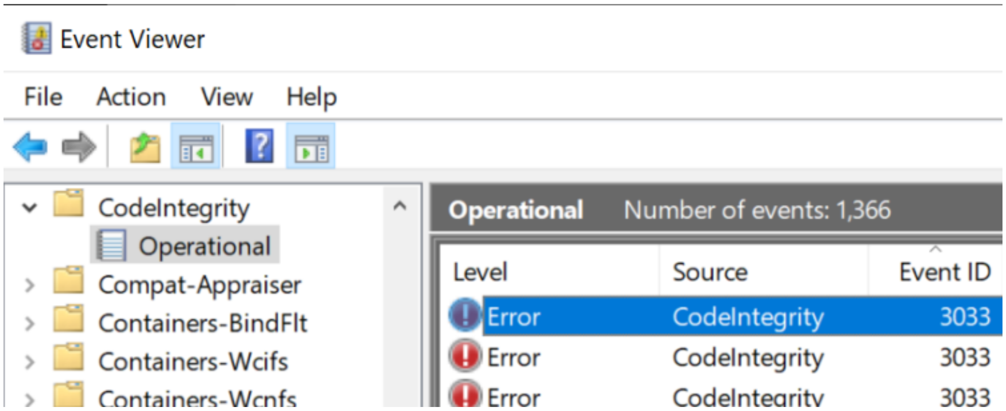
Navigate your browser to the URL **chrome://conflicts#R** to show the list of modules loaded by the client. Look for any files that are not **Signed By** Microsoft or Google.

If you see any, they are *suspects*. (There will likely be a few listed as `Shell Extensions`; e.g. 7-Zip.dll, that *do not* cause this problem)– check for an **R** in the **Process types** column to find modules loading in the Renderers.

You should install any available updates for any of your *suspects* to see if doing so fixes the problem.

Check the Event Log

The Windows Event Log will contain information about modules denied loading. Open **Event Viewer**. Expand **Applications and Services Logs** > **Microsoft** > **Windows** > **CodeIntegrity** > **Operational** and look for events with ID **3033**. The detail information will indicate the name and location of the DLL that caused the crash:



Operational Number of events: 1,366

Level	Source	Event ID
Error	CodeIntegrity	3033
Error	CodeIntegrity	3033
Error	CodeIntegrity	3033

Optional: Use Enterprise Policy to disable the new protection

If needed, IT Adminstrators can disable the new protection using the RendererCodeIntegrity policy for Chrome and Edge. You should outreach to the software vendors responsible for the problematic applications and request that they update them.

Other possible causes

Note that it's possible that you could have a PC that encounters symptoms like this (all subprocesses crash) but *not* a result of the new code integrity check. In such cases, the Error Code on the crash page will be something *other* than STATUS_INVALID_IMAGE_HASH.

- For instance, Chromium once had **an obscure bug** in its sandboxing code that caused all sandboxes to crash depending on the random memory mapping of Address Space Layout Randomization.
- Similarly, Chrome and Edge still have **an active bug** where all renderers crash on startup if the PC has AppLocker enabled and the browser is launched elevated (as Administrator).

-Eric

Share this:

Twitter Facebook

ericlaw **2019-09-27** **browsers**, **security**, **web**
Chrome, **debugging**, **Edge**, **security**, **troubleshooting**

Published by ericlaw

Impatient optimist. Dad. Author/speaker. Created Fiddler & SlickRun. PM @ MSFT '01-'12, and '18-, presently working on Microsoft Edge. My words are my own. **View more posts**

18 thoughts on "Aw, snap! What if Every Tab Crashes?"

Jeff
2019-09-30 at 12:40

Thanks for the info. Here's what I found after going to the edge://conflicts. The are only 3 that weren't signed by MS or Google. All are up to date. Figured I'd pass the info on in hopes that it will help find the problem.

Symantec CMC Firewall sysfer Symantec Corporation sysfer.dll 5A1ADC9695000 BR %systemroot%\system32\ sysfer.dll

Radeon Settings: Desktop Control Panel Advanced Micro Devices, Inc. atiacm64.dll 5D781A1616c000 None %programfiles%\amd\cnext\cnext\ atiacm64.dll (Shell extension)

Adobe Acrobat Context Menu Adobe Systems, Incorporated contextmenushim64.dll 5507CE7E289000 None c:\program files (x86)\adobe\acrobat 2015\acrobat elements\ contextmenushim64.dll (Shell extension)

Reply

ericlaw
2019-10-02 at 17:46

The Symantec DLL is your culprit here; note that it’s got an “R” (meaning Renderer). I’m not sure how you determined that it’s “up-to-date”: What version of Symantec Endpoint Protection do you have installed?

Reply

brucedawson
2019-10-25 at 16:48

The first eight digits after the DLL name are the build time-stamp in hexadecimal. 5A1ADC96 translates to 2017-11-26 07:24:06 so you have a very old DLL.

Shshid
2020-05-17 at 07:04

It shows location like this in error, really annoying
Device\HarddiskVolume5\Windows\System 32\winhafnt64.dll

Reply

Rameez Zafar
2020-05-17 at 14:39

Alright I followed each step. Found many events with the ID 3033. It basically says that “code integrity determined that a process*file name* attempted to load *file name* that did not meet the Microsoft signing level requirements.” What to do next?

Reply

ericlaw
2020-05-17 at 15:19

The filename tells you the problem file. Write it here and we can figure it out.

Reply

Rameez Zafar
2020-05-17 at 19:05

Oh and there was only one non-microsoft signed module in edge://conflicts/#R and it's this: Symantec CMC Firewall sysfer Symantec Corporation 12.1.7004.6500 576A283789000 BR %systemroot%\system32\ sysfer.dll

Reply

ericlaw
2020-05-17 at 22:33

And there's your answer– you are running the outdated version of Symantec that is not compatible with RendererCodeIntegrity. You will need to install the update from Symantec.

Reply

Rameez Zafar
2020-05-18 at 01:14

But i did the LiveUpdate just before that. It says that there are no updates available. How do i update it further or properly?

ericlaw
2020-05-18 at 13:58

I'm afraid that's a question for Symantec Support. Perhaps their Knowledge Base article will be helpful: https://knowledge.broadcom.com/external/article?legacyId=tech256047

Rameez Zafar
2020-05-18 at 19:16

Alright. Thank you very much for the explanation and help. I am embarrassed to admit how long I have been browser-less.

Reply

AndrewEstes
2020-06-27 at 12:18

LiveUpdate does not always update the Symantec program itself. Mostly LiveUpdate is for virus definitions. It's best to do a reinstall from an up-to-date source.

Reply

Derek
2020-08-10 at 13:45

I believe that my issue here is with winhafnt64.dll : Code Integrity determined that a process (\Device\HarddiskVolume4\Program Files (x86)\Microsoft\Edge\Application\msedge.exe) attempted to load \Device\HarddiskVolume4\Windows\System32\winhafnt64.dll that did not meet the Microsoft signing level requirements.

I cannot find out any details of this program or what it does or how to update. Any advice?

Reply

ericlaw
2020-08-10 at 18:24

A few searches suggest that this DLL is a part of a (corporate) spyware package used to monitor computers; see **https://www.shouldiremoveit.com/surveilstar3-109642-program.aspx** for instance.

Reply

Derek
2020-08-11 at 06:29

Thats what I was afraid of, not much I can do about it. Chrome works just fine but i can't use the new edge. Thanks

ericlaw
2020-08-11 at 13:38

Are you /expecting/ this machine to be running spyware?

Chrome has the same RendererCodeIntegrity feature as Edge does and should crash in exactly the same way. Do you see this DLL in the chrome://conflicts page?

Derek

2020-08-11 at 13:48

It is a company computer, using a corporate antivirus package so I don't see it being a dangerous spyware deal. I would imagine they have some way of tracking computer usage with such a program. I have been using chrome just fine since day 1, but was having problems with some program running that I have since got fixed, but was asked to open it using edge, and edge would not open, just crashed. I tried uninstalling and reinstalling and the same thing happens, but chrome still works fine.

ericlaw
2020-08-11 at 13:57

Ah. You may wish to discuss this with your IT department just to confirm that the DLL is expected. If Chrome is working, and you see this DLL in Chrome's conflicts list, that suggests that your IT Administrator has set a Chrome policy that disables the security feature. That same policy is available for Edge; see **https://docs.microsoft.com/en-us/deployedge/microsoft-edge-policies#renderercodeintegrityenabled**

Leave a Reply

Enter your comment here...

text/plain, **A WordPress.com Website**.