Google tested the top 5 browsers, Safari results with the most security flaws

The Project Zero team in Google has just created a browser engine DOM testing tool and tested the top 5 browsers today. The results show that Apple's Safari browser has a lot of errors.

The Project Zero team in Google has just created a browser engine DOM testing tool and tested the top 5 browsers today. The results show that Apple's Safari browser has a lot of errors.

The tool called Domato is a security toolkit, using random data and analyzing the output to find anomalies. Google's engineer Ivan Fratric created Domato with the goal of detecting the DOM engine's error, a browser element used to read HTML and arrange in the DOM (Document Object Model), then display within the browser Users still see on the screen.

Google: errors on the DOM engine need to be prioritized

Fratric said he focused on the DOM engine because 'rarely did anyone release security updates that didn't contain at least some errors on the DOM engine'. Although Flash errors appear in many browsers, when Flash goes away (by 2020), the attacker will focus on the DOM engine. For Domato, he hopes to help check and patch security issues related to the DOM engine before it's too late.

Discover 17 security bugs in Safari's DOM engine

To demonstrate, Fratric performed tests on five popular browsers Chrome, Firefox, Internet Explorer, Edge and Safari, bringing in 100 million fuzz tests.

The results show that Safari has the most errors with 17 bugs. Behind with Edge with 6 bugs, IE and Firefox have 4 bugs and Chrome only has 2 errors. Not counting errors that are not confidential.

Fratric also pointed out that if Microsoft does not add MemGC (preventing UAF security holes) on IE and Edge, their results will be much worse.

Supplier
Browser
Engine
Error number
Project Zero Bug IDs
Google
Chrome
Blink

2
994, 1024
Mozilla
Firefox
Gecko
4 *
1130, 1155, 1160, 1185
Microsoft
Internet Explorer
Trident
4
1011, 1076, 1118, 1233
Microsoft
Edge
EdgeHtml
6
1011, 1254, 1255, 1264, 1301, 1309
Apple
Safari
WebKit
17
999, 1038, 1044, 1080, 1082, 1087, 1090, 1097, 1105, 1114, 1241, 1242, 1243, 1244, 1246, 1249, 1250
total
thirty first**

** Total is 33 but there are 2 errors affecting many browsers.*
*** One of the errors found in Firefox is on the Skia graphics library, not in Firefox's source code. But code errors are contributed by Mozilla engineers to Skia.*

Google said it had informed the parties about new errors discovered and included a copy of Domato to enable them to check further. Fratric also puts Domato source code on GitHub https://github.com/google/domato and hopes others will use it to work on other applications, not just the browser DOM engine. Domato is also not the only tool of Google to detect security flaws, before it also had OSS Fuzz and syzkaller.