**Table of Contents**

Introduction...................................................I

Purpose.......................................................................................................... II

Scope .....................................................................................III Results......................................................................................................................IV

Conclusion.............................................................................................................V

References and Links..........................................................................................................VI

Key Terms.............................................................................................................................VII

**I.** **Introduction**

The purpose of this report is to provide an analysis of web browser vulnerabilities for three popular browsers: Mozilla Firefox, Microsoft Edge, and Apple Safari. The report aims to differentiate and compare the vulnerabilities associated with each browser, ultimately offering recommendations to users based on the findings. This assessment has been conducted by gathering information from the CVE Details website (<https://www.cvedetails.com/>), which is a comprehensive database of known vulnerabilities.

**II. Purpose**

The purpose of this report is to enhance the understanding of web browser vulnerabilities and assist users in making informed decisions regarding their choice of browser. By examining the vulnerabilities present in Mozilla Firefox, Microsoft Edge, and Apple Safari, we can identify potential risks and recommend the most secure browser option for users.

**III. Scope**

For this assessment, information was collected from the CVE Details website, which provides an extensive list of vulnerabilities for various software products, including web browsers. The focus was specifically on Mozilla Firefox, Microsoft Edge, and Apple Safari. The assessment covers vulnerabilities that have been identified since 2017 up to 2023. The analysis focused on a few known vulnerabilities common across all browsers.

**IV. Results**

1. Mozilla Firefox:

According to the CVE Details website, Mozilla Firefox has encountered a significant number of vulnerabilities in recent years. These vulnerabilities encompass various areas such as memory corruption, cross-site scripting (XSS), and remote code execution. Firefox's open-source nature and extensive plugin ecosystem have made it a target for attackers seeking to exploit vulnerabilities in these areas.

One noteworthy vulnerability in Firefox is CVE-2021-29953, which allowed for arbitrary code execution through maliciously crafted web content. Mozilla promptly released patches to address this vulnerability and continues to demonstrate a proactive approach to security.



1. Microsoft Edge:

Microsoft Edge, the successor to Internet Explorer, has made significant strides in terms of security. By adopting the Chromium engine, Edge benefits from the continuous security improvements made by the Chromium project. However, vulnerabilities specific to Edge still exist.

Among the vulnerabilities reported for Microsoft Edge, one example is CVE-2020-1020, a memory corruption flaw that could be exploited to execute arbitrary code. Microsoft has demonstrated a commitment to addressing such vulnerabilities promptly and releasing patches to ensure user safety.



1. Apple Safari:

Safari, the default web browser for Apple devices, has generally been regarded as a secure browser due to Apple's emphasis on security measures. However, it has not been without vulnerabilities.

CVE-2020-9982 is one such vulnerability that impacted Safari. It allowed attackers to execute arbitrary code through maliciously crafted web content. Apple has been diligent in releasing security updates and patches to mitigate these vulnerabilities.





**V. Conclusion**

Safari remains a solid choice for users of Apple devices. It is the least targeted and its vulnerabilities are generally addressed swiftly through security updates. Second is Edge with minor attacks over the years.

No matter what your choice, it is crucial to consider regular software updates to minimize attack risks and to meet the company’s privacy and security measures.

**VI. References and Links**

* CVE Details, retrieved from <https://www.cvedetails.com/>
* Starting out with C++ from Control Structures to Objects ,10th edition, Tony Gaddis
* Network Security Essentials, Ahmed F. Sheikh Miami, FL, USA

**VII. Key terms**

**Denial-of-Service Attack**

This networks attack is to deny access to authorized users by making the network unavailable. The attackers overwhelm a target by too many requests until the system can’t handle processing those packets.

**Execute Code**

Malicious code or program designed to disrupt computer operation or to gain access to computer systems without the user’s knowledge or permission.

**Buffer Overflows**

Overflow is a vulnerability that results in poor coding practices and memory management. A program accepts more input than it has assigned storage space.

**Memory corruption**

It refers to any unwanted modification of data in a program's memory, which can occur due to software bugs, programming errors, or malicious activities.

**By: Didier Niyomukiza**