Cross Site Scripting vulnerability when using AdGuard Application v.7.18.1 (4778) and before allows an attacker to execute arbitrary code via a crafted payload to the fontMatrix component.

@ChiampionDuck (https://github.com/VuDuc09)

Overview

Vulnerability Type	Cross Site Scripting (XSS)
Affected System	Web Applications have PDF Preview function when user enable HTTPS filtering in AdGuard (Filters HTTPS protocol in AdBlock Ultimate)

Description

This report outlines a vulnerability in the AdGuard application when users enable the HTTPS filtering function and access a web application with the PDF preview feature. By exploiting this vulnerability, an attacker can use the techniques described in CVE-2024-4367 to create an XSS attack to steal user information or hijack the login session.

Vulnerability Details

Evironment Settings

AdGuard Windows Application v.7.18.1 (4778) and AdGuard Browser Extension

AdBlock Ultimate Windows Application v.4.3.8 and AdBlock Ultimate Browser Extension

Browser: Microsoft Edge 128.0.2739.79, Arc Browser 1.1.1.27314 (0000), Chrome 128.0.6613.138, Vivaldi 6.9.3447.46, Firefox 115.14.0esr

OS: Windows 11 Pro 10.0.26100 Build 26100

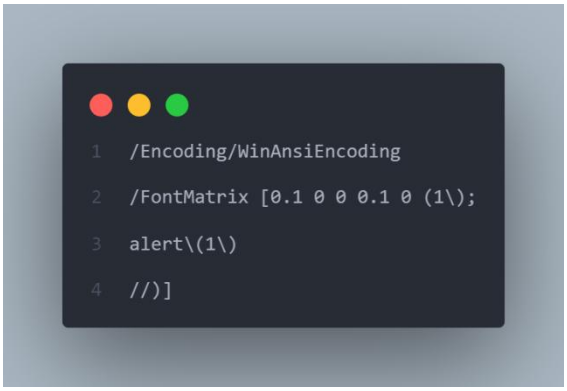
Web Application (Censored domain because security reasons): *X.vn*

Web Application Function

X.vn have *dam-test.X.vn* subdomains to file management and *dam-api-test.X.vn* subdomains that *dam-test.X.vn* call to preview files.

Proof of Concept

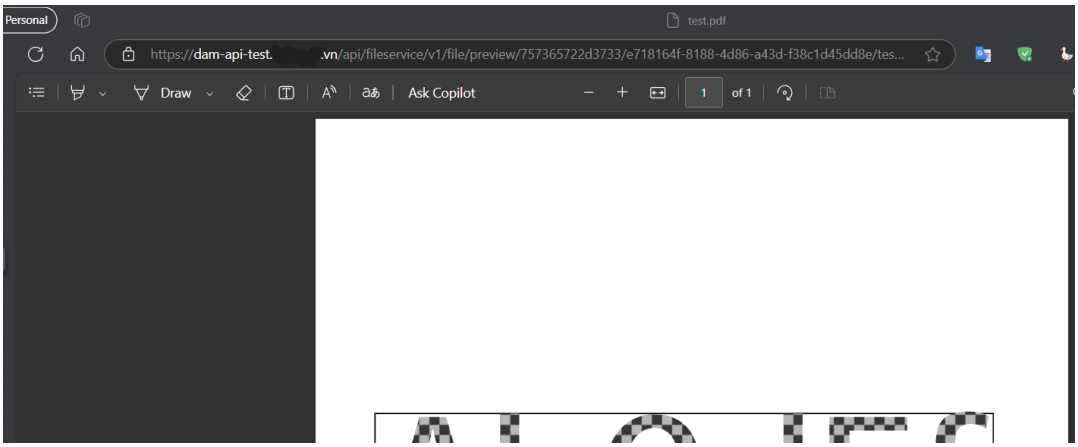
1. Create a PDF file and injection a JS script in FontMatrix



2. Check that the functions of the website that work properly without vulnerability when disabling HTTPS filtering in AdGuard (Filters HTTPS protocol in AdBlock Ultimate)

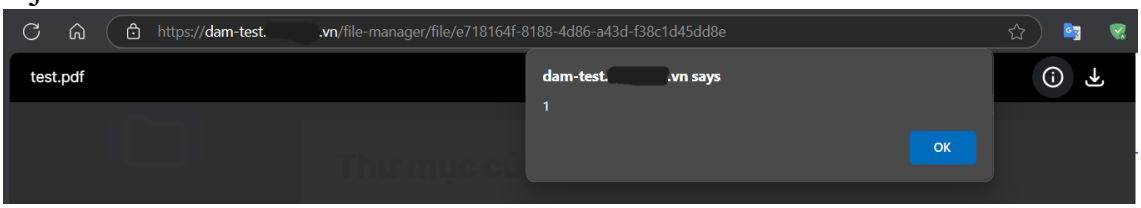
- Preview malicious PDF file in *dam-test.X.vn*

- Access direct PDF file in *dam-api-test.X.vn*

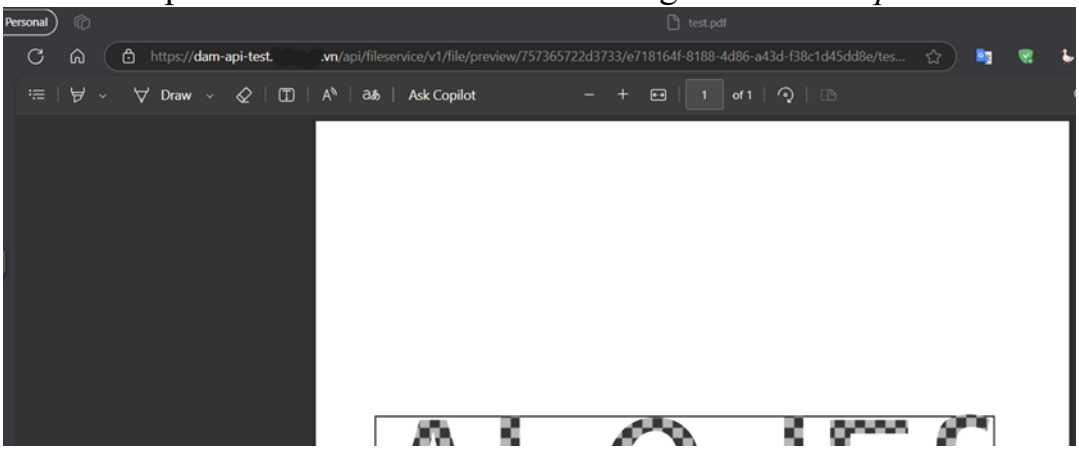


3. When HTTPS filtering on AdGuard (Filters HTTPS protocol in AdBlock Ultimate) is enabled

- Preview malicious PDF file in *dam-test.X.vn* can execute a JS script that are injected into it



- But JS script doesn't execute when accessing direct *dam-api-test.X.vn*



4. Check header of response packets

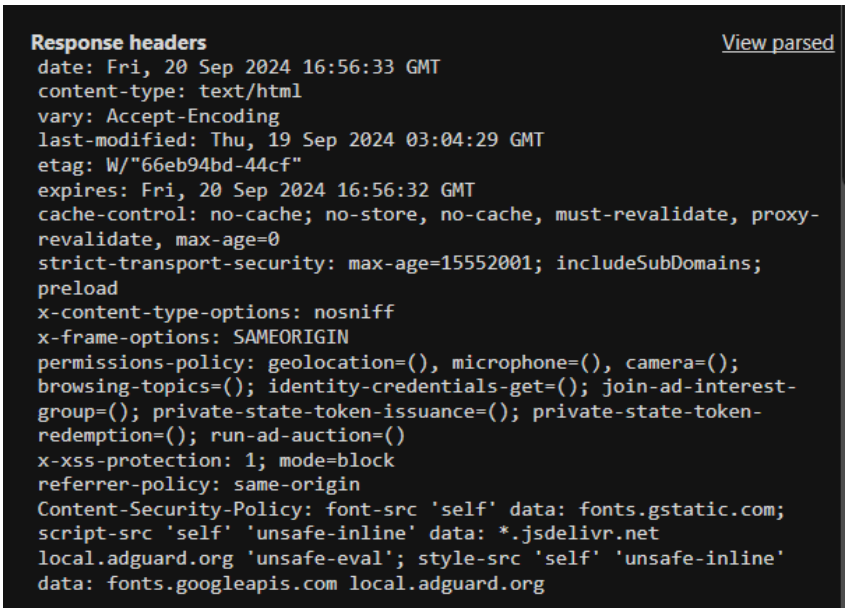
- Response packets of the *dam-test.X.vn* when accessing the file manager function

```
HTTP/2 200 OK
Date: Sat, 21 Sep 2024 15:41:51 GMT
Content-Type: text/html
Vary: Accept-Encoding
Last-Modified: Thu, 19 Sep 2024 03:04:29 GMT
Etag: W/"66eb94bd-44cf"
Expires: Sat, 21 Sep 2024 15:41:50 GMT
Cache-Control: no-cache
Cache-Control: no-store, no-cache, must-revalidate,
proxy-revalidate, max-age=0
Content-Security-Policy: script-src 'self' 'unsafe-inline' data:
*.jsdelivr.net; style-src 'self' 'unsafe-inline' data:
fonts.googleapis.com; font-src 'self' data: fonts.gstatic.com;
Strict-Transport-Security: max-age=15552001; includeSubDomains;
preload
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Permissions-Policy: geolocation=(), microphone=(), camera=()
X-Xss-Protection: 1; mode=block
Referrer-Policy: same-origin
```

Normal response header

content-security-policy	script-src 'self' 'unsafe-inline' data: *.jsdelivr.net self.adblockultimate.net 'unsafe-eval'; style-src 'self' 'unsafe-inline' data: fonts.googleapis.com self.adblockultimate.net; font-src 'self' data: fonts.gstatic.com
content-type	text/html
date	Wed, 09 Oct 2024 02:15:29 GMT
etag	W/"66eb94bd-44cf"
expires	Wed, 09 Oct 2024 02:15:28 GMT
last-modified	Thu, 19 Sep 2024 03:04:29 GMT
permissions-policy	geolocation=(), microphone=(), camera=()
referrer-policy	same-origin
strict-transport-security	max-age=15552001; includeSubDomains; preload
vary	Accept-Encoding
x-abu-active	true
x-abu-version	AdBlocker Ultimate for Windows;4.3.8;Windows
x-abu-windows-version	4.3.8
x-content-type-option	nosniff

Header when using Filters HTTPS protocol in AdBlock Ultimate

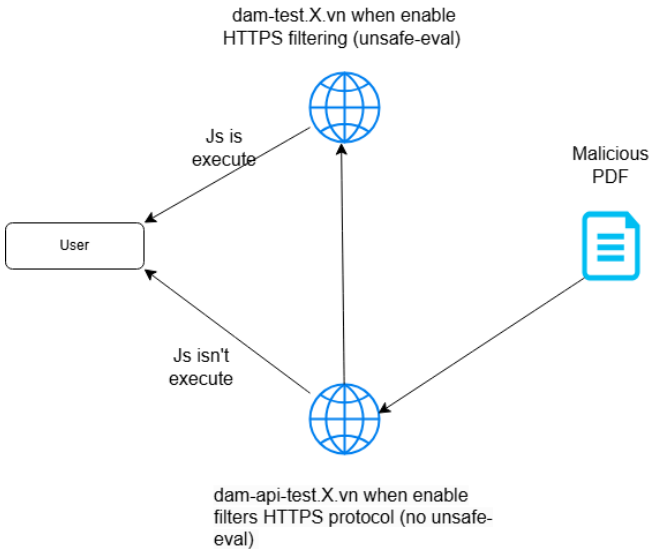


Header when using HTTPS filtering in AdGuard

- The difference occurs in the CSP header of the packet AdGuard and AdBlock Ultimate returns when accessing *dam-test.X.vn* with the *unsafe-eval* of *script-src* parameter appearing (Inside this header there is also the appearance of local.adguard.org (self.adblockultimate.net) which acts as a proxy to better block ads – the HTTPS filtering (filters HTTPS protocol) function).

5. Vulnerable description

- A JS script is injected into FontMatrix can be executed when Web Application enable the *eval()* feature in preview PDF files. The *eval()* feature has been disabled in the latest PDF previewers (e.g., PDF.js).
- In this environment, when calling PDF files directly from *dam-api-test.X.vn* there are no security issues. But when previewing the file via *dam-test.X.vn*, AdGuard and Adblock Ultimate added the unsafe-eval parameter (this parameter allows running commands inside eval()) and a security error occurred for users when accessing malicious files.



- After tests, websites that use the 'unsafe-inline' parameter in the SCP header when requests go through AdGuard and Adblock Ultimate will have the 'unsafe-eval' parameter patched.

Potential Impact

- The JS script injected can exfiltrate data or install malware on the user's machine. Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.
- Impact on AdGuard's and Adblock Ultimate's reputation when users are exposed to XSS attacks when using there apps, which they would not be affected when accessing the website normally.
- May involve legal issues affecting users and web application providers

Affected Applications

- AdGuard Windows Application v.7.18.1 (4778) and before
- Adblock Ultimate Windows Application v.4.3.8 and before

Mitigations

- Keep the parameters in the csp header of the web application intact, avoid adding dangerous parameters such as *'unsafe-inline'* and *'unsafe-eval'* by default
- Adjust the syntax of the rules, especially with security-related headers
- Update to the latest version of ad blockers (AdGuard Windows Application v.7.19 or higher, Adblock Ultimate Windows Application v4.3.9 or higher)

Conclusion

Cross Site Scripting vulnerability when using AdGuard Application v.7.18.1 (4778) and AdBlock Ultimate v.4.3.8 are critical and poses significant risks due to the potential exposure of exfiltrated data, installing malware, hijacking sessions, and legal issues. Immediate action should be taken to protect against this type of attack.