Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică si Microelectronica

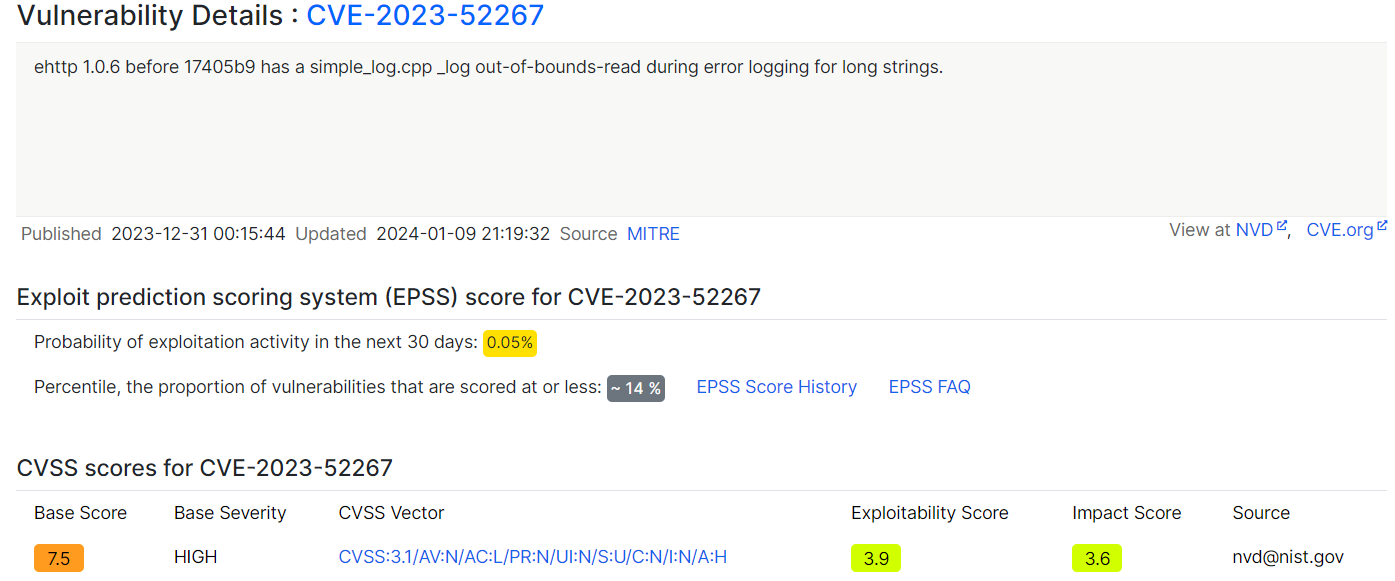
Specialitatea: Securitate Informațională

**Lucrul individual**   
 Managementul si Auditul Securitati Informationale

A elaborat : Chihai Adrian   
A verificat : Bulai Rodica

Chișinău 2024

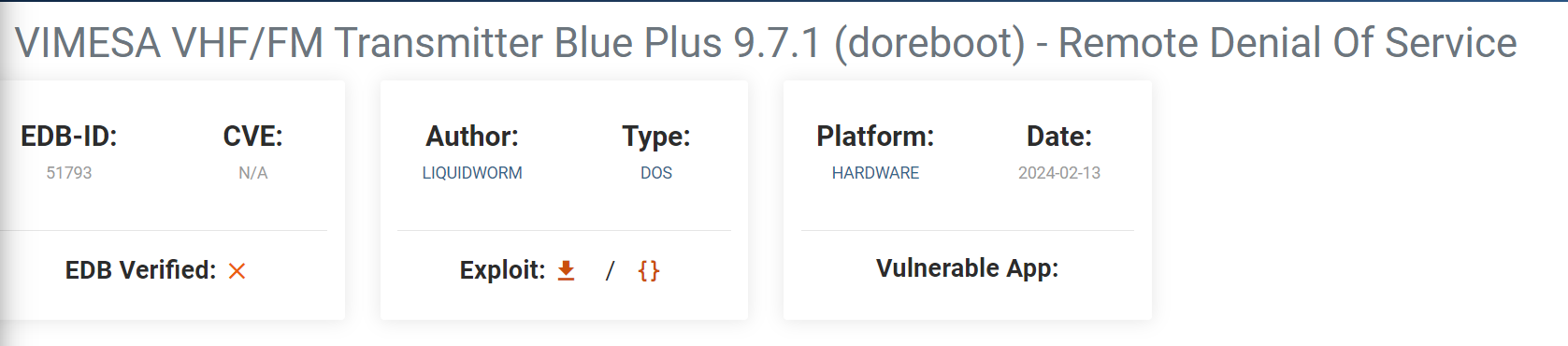
1.https://www.cvedetails.com/cve/CVE-2021-45907/  
CVE-2021-45907 este o vulnerabilitate în gif2apng 1.9, implicând un overflow al buffer-ului bazat pe stivă într-o buclă for. Atacatorul are o influență limitată asupra datelor scrise pe stivă, ceea ce face puțin probabilă subminarea fluxului de control. Scorurile CVSS indică o severitate medie până la ridicată, cu posibilitatea unui impact parțial sau complet asupra confidențialității, integrității și disponibilității datelor.



2.<https://www.exploit-db.com/>

Dispozitivul suferă de o vulnerabilitate de Denial of Service (DoS). Un atacator neautentificat poate emite o solicitare HTTP GET neautorizată către punctul final neprotejat 'doreboot' și poate reporni operațiile transmițătorului.

Această vulnerabilitate poate fi folosită de către atacatori pentru a perturba funcționarea normală a transmițătorului, ceea ce poate duce la întreruperi în transmiterea semnalului și la alte probleme legate de operarea dispozitivului.



3.https://www.rapid7.com/db/vulnerabilities/mfsa2024-05-cve-2024-1546/  
În Firefox 123 și versiunile anterioare, inclusiv Firefox ESR 115.8 și Thunderbird 115.8, a fost identificată o vulnerabilitate de securitate. Aceasta se referă la o confuzie a lungimii bufferelor în timpul stocării și re-accesării datelor pe un canal de rețea, ceea ce poate duce la o citire a memoriei în afara limitelor.

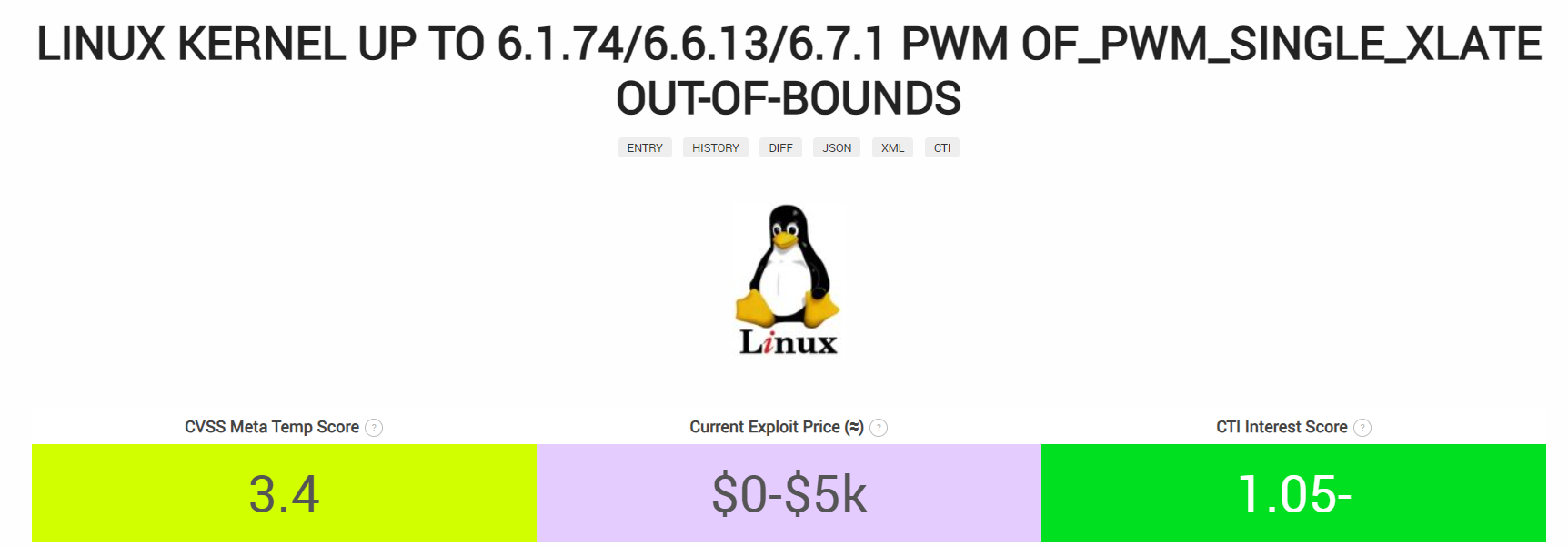
Soluție:

Actualizarea la versiunea 123 a Firefox sau la o versiune ulterioară. De exemplu, soluția specificată este "mozilla-firefox-upgrade-123\_0". Este recomandabil să se efectueze această actualizare cât mai curând posibil pentru a remedia vulnerabilitatea și pentru a menține securitatea navigării pe internet.



4.<https://vuldb.com/>

Este vorba despre o vulnerabilitate considerată problematică, clasificată ca fiind o vulnerabilitate de tip out-of-bounds în funcția of\_pwm\_single\_xlate a componentei pwm. CWE (Common Weakness Enumeration) clasifică problema ca fiind CWE-125, care indică faptul că produsul citește date dincolo de sfârșitul sau începutul bufferului intenționat, având un impact asupra confidențialității. Utilizatorilor li se sugerează să upgradeze la cea mai recentă versiune disponibilă pentru a elimina această vulnerabilitate.



5.https://nvd.nist.gov/vuln/detail/CVE-2022-3479

Vulnerabilitatea CVE-2022-3479 afectează NSS (Network Security Services), un set de biblioteci utilizate pentru implementarea securității în aplicații software. Iată detalii despre această problemă de Securitate. Este vorba despre o vulnerabilitate găsită în NSS, care poate duce la o cădere a autentificării clientului fără un certificat de utilizator în baza de date. Acest lucru poate duce la o eroare de segmentare sau la o cădere a sistemului.

