## **1. JQuery 1.2 < 3.5.0 Multiple XSS**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D001** | ORTA SEVİYE |
| **Bulgu Adı** | JQuery 1.2 < 3.5.0 Multiple XSS |
| **CVE Kodu** | CVE-2020-11022, CVE-2020-11023 |
| **CVSS Skoru** | 4.3 | CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N |
| **Bulgu Türü** | Güvenlik Zafiyeti |
| **Bulgu Detayı** | Yapılan güvenlik testleri sonucunda ilgili sistemlerde belirtilen güvenlik zafiyetlerine rastlanmıştır.  *Şekil : Güvenlik zafiyeti tespitine yönelik ekran görüntüsü*  **NOT:** Ekran görüntüleri örneklem olarak paylaşılmıştır. Diğer sistemleri görmek için etkilenen bileşenlere bakınız. |
| **Erişim Noktası** | İnternet |
| **Kullanıcı Profili** | Anonim Kullanıcı |
| **Etkilenen Bileşenler** | 172.30.141.15:3000/tcp |
| **Bulgu Açıklaması** | According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.  Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release. |
| **Çözüm Önerisi** | Upgrade to JQuery version 3.5.0 or later. |
| **İlgili Bağlantılar** | https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-SA-2020-0007 |

## **2. SMB Signing not required**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D002** | ORTA SEVİYE |
| **Bulgu Adı** | SMB Signing not required |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | 5.0 | CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N |
| **Bulgu Türü** | Güvenlik Zafiyeti |
| **Bulgu Detayı** | Yapılan güvenlik testleri sonucunda ilgili sistemlerde belirtilen güvenlik zafiyetlerine rastlanmıştır.  *Şekil : Güvenlik zafiyeti tespitine yönelik ekran görüntüsü*  **NOT:** Ekran görüntüleri örneklem olarak paylaşılmıştır. Diğer sistemleri görmek için etkilenen bileşenlere bakınız. |
| **Erişim Noktası** | İnternet |
| **Kullanıcı Profili** | Anonim Kullanıcı |
| **Etkilenen Bileşenler** | 172.30.141.15:445/tcp |
| **Bulgu Açıklaması** | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. |
| **Çözüm Önerisi** | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| **İlgili Bağlantılar** | http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea |

## **3. ICMP Timestamp Request Remote Date Disclosure**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D003** | DÜŞÜK SEVİYE |
| **Bulgu Adı** | ICMP Timestamp Request Remote Date Disclosure |
| **CVE Kodu** | CVE-1999-0524 |
| **CVSS Skoru** | 2.1 | CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N |
| **Bulgu Türü** | Güvenlik Zafiyeti |
| **Bulgu Detayı** | Yapılan güvenlik testleri sonucunda ilgili sistemlerde belirtilen güvenlik zafiyetlerine rastlanmıştır.  *Şekil : Güvenlik zafiyeti tespitine yönelik ekran görüntüsü*  **NOT:** Ekran görüntüleri örneklem olarak paylaşılmıştır. Diğer sistemleri görmek için etkilenen bileşenlere bakınız. |
| **Erişim Noktası** | İnternet |
| **Kullanıcı Profili** | Anonim Kullanıcı |
| **Etkilenen Bileşenler** | 172.30.141.15:0/icmp |
| **Bulgu Açıklaması** | The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.  Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time. |
| **Çözüm Önerisi** | Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |