## **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. |

## **4. Nessus SYN scanner**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D004** | BİLGİLENDİRME |
| **Bulgu Adı** | Nessus SYN scanner |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:49671/tcp 172.30.141.15:49669/tcp 172.30.141.15:49668/tcp 172.30.141.15:49667/tcp 172.30.141.15:49666/tcp 172.30.141.15:49665/tcp 172.30.141.15:49664/tcp 172.30.141.15:6000/tcp 172.30.141.15:5900/tcp 172.30.141.15:5800/tcp 172.30.141.15:5040/tcp 172.30.141.15:3000/tcp 172.30.141.15:445/tcp 172.30.141.15:139/tcp 172.30.141.15:135/tcp |
| **Bulgu Açıklaması** | This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.   Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded. |
| **Çözüm Önerisi** | Protect your target with an IP filter. |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **5. DCE Services Enumeration**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D005** | BİLGİLENDİRME |
| **Bulgu Adı** | DCE Services Enumeration |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:49671/tcp 172.30.141.15:49669/tcp 172.30.141.15:49668/tcp 172.30.141.15:49667/tcp 172.30.141.15:49666/tcp 172.30.141.15:49665/tcp 172.30.141.15:49664/tcp 172.30.141.15:445/tcp 172.30.141.15:135/tcp |
| **Bulgu Açıklaması** | By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **6. VNC Server Unencrypted Communication Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D006** | BİLGİLENDİRME |
| **Bulgu Adı** | VNC Server Unencrypted Communication Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5900/tcp |
| **Bulgu Açıklaması** | This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **7. VNC Server Security Type Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D007** | BİLGİLENDİRME |
| **Bulgu Adı** | VNC Server Security Type Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5900/tcp |
| **Bulgu Açıklaması** | This script checks the remote VNC server protocol version and the available 'security types'. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **8. VNC Software Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D008** | BİLGİLENDİRME |
| **Bulgu Adı** | VNC Software Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5900/tcp |
| **Bulgu Açıklaması** | The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another. |
| **Çözüm Önerisi** | Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port. |
| **İlgili Bağlantılar** | https://en.wikipedia.org/wiki/Vnc |

## **9. Service Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D009** | BİLGİLENDİRME |
| **Bulgu Adı** | Service Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5900/tcp 172.30.141.15:5800/tcp 172.30.141.15:3000/tcp |
| **Bulgu Açıklaması** | Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **10. HyperText Transfer Protocol (HTTP) Information**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D010** | BİLGİLENDİRME |
| **Bulgu Adı** | HyperText Transfer Protocol (HTTP) Information |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5800/tcp 172.30.141.15:3000/tcp |
| **Bulgu Açıklaması** | This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...   This test is informational only and does not denote any security problem. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **11. UltraVNC Java Viewer Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D011** | BİLGİLENDİRME |
| **Bulgu Adı** | UltraVNC Java Viewer Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5800/tcp |
| **Bulgu Açıklaması** | UltraVNC Java Viewer, a VNC server viewer, is accessible through the remote web server. |
| **Çözüm Önerisi** | Make sure that use of this program is in accordance with your organization's acceptable use and security policies. |
| **İlgili Bağlantılar** | http://www.uvnc.com/ |

## **12. VNC HTTP Server Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D012** | BİLGİLENDİRME |
| **Bulgu Adı** | VNC HTTP Server Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:5800/tcp |
| **Bulgu Açıklaması** | The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another. |
| **Çözüm Önerisi** | Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port. |
| **İlgili Bağlantılar** | https://en.wikipedia.org/wiki/Vnc |

## **13. JQuery Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D013** | BİLGİLENDİRME |
| **Bulgu Adı** | JQuery Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | Nessus was able to detect JQuery on the remote host. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | https://jquery.com/ |

## **14. Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D014** | BİLGİLENDİRME |
| **Bulgu Adı** | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **15. Microsoft Windows SMB Versions Supported (remote check)**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D015** | BİLGİLENDİRME |
| **Bulgu Adı** | Microsoft Windows SMB Versions Supported (remote check) |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.  Note that this plugin is a remote check and does not work on agents. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **16. Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D016** | BİLGİLENDİRME |
| **Bulgu Adı** | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues. |
| **Çözüm Önerisi** | Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices. |
| **İlgili Bağlantılar** | https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and http://www.nessus.org/u?8dcab5e4 http://www.nessus.org/u?234f8ef8 http://www.nessus.org/u?4c7e0cf3 |

## **17. WMI Not Available**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D017** | BİLGİLENDİRME |
| **Bulgu Adı** | WMI Not Available |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.  Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page |

## **18. Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D018** | BİLGİLENDİRME |
| **Bulgu Adı** | Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | It was not possible to connect to PIPE\winreg on the remote host.  If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **19. Microsoft Windows SMB NativeLanManager Remote System Information Disclosure**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D019** | BİLGİLENDİRME |
| **Bulgu Adı** | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **20. Microsoft Windows SMB Service Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D020** | BİLGİLENDİRME |
| **Bulgu Adı** | Microsoft Windows SMB Service Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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 172.30.141.15:139/tcp |
| **Bulgu Açıklaması** | The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **21. Windows NetBIOS / SMB Remote Host Information Disclosure**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D021** | BİLGİLENDİRME |
| **Bulgu Adı** | Windows NetBIOS / SMB Remote Host Information Disclosure |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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** | 172.30.141.15:137/udp |
| **Bulgu Açıklaması** | The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.  Note that this plugin gathers information to be used in other plugins, but does not itself generate a report. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **22. Traceroute Information**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D022** | BİLGİLENDİRME |
| **Bulgu Adı** | Traceroute Information |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/udp |
| **Bulgu Açıklaması** | Makes a traceroute to the remote host. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **23. OS Security Patch Assessment Not Available**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D023** | BİLGİLENDİRME |
| **Bulgu Adı** | OS Security Patch Assessment Not Available |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | OS Security Patch Assessment is not available on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.  This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **24. Nessus Scan Information**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D024** | BİLGİLENDİRME |
| **Bulgu Adı** | Nessus Scan Information |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | This plugin displays, for each tested host, information about the scan itself :   - The version of the plugin set.  - The type of scanner (Nessus or Nessus Home).  - The version of the Nessus Engine.  - The port scanner(s) used.  - The port range scanned.  - The ping round trip time   - Whether credentialed or third-party patch management checks are possible.  - Whether the display of superseded patches is enabled  - The date of the scan.  - The duration of the scan.  - The number of hosts scanned in parallel.  - The number of checks done in parallel. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **25. Common Platform Enumeration (CPE)**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D025** | BİLGİLENDİRME |
| **Bulgu Adı** | Common Platform Enumeration (CPE) |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.   Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | http://cpe.mitre.org/ https://nvd.nist.gov/products/cpe |

## **26. Patch Report**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D026** | BİLGİLENDİRME |
| **Bulgu Adı** | Patch Report |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.  Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled. |
| **Çözüm Önerisi** | Install the patches listed below. |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **27. Target Credential Status by Authentication Protocol - No Credentials Provided**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D027** | BİLGİLENDİRME |
| **Bulgu Adı** | Target Credential Status by Authentication Protocol - No Credentials Provided |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.  Please note the following :  - This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.  - Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **28. Device Type**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D028** | BİLGİLENDİRME |
| **Bulgu Adı** | Device Type |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc). |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **29. OS Identification**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D029** | BİLGİLENDİRME |
| **Bulgu Adı** | OS Identification |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |

## **30. Ethernet Card Manufacturer Detection**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D030** | BİLGİLENDİRME |
| **Bulgu Adı** | Ethernet Card Manufacturer Detection |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | https://standards.ieee.org/faqs/regauth.html http://www.nessus.org/u?794673b4 |

## **31. Ethernet MAC Addresses**

|  |  |
| --- | --- |
| **PT-TEST-2025-06-D031** | BİLGİLENDİRME |
| **Bulgu Adı** | Ethernet MAC Addresses |
| **CVE Kodu** | CVE bilgisi mevcut değil |
| **CVSS Skoru** | Skor bilgisi mevcut değil |
| **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/tcp |
| **Bulgu Açıklaması** | This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list. |
| **Çözüm Önerisi** | n/a |
| **İlgili Bağlantılar** | İlgili bağlantı bilgisi mevcut değil. |