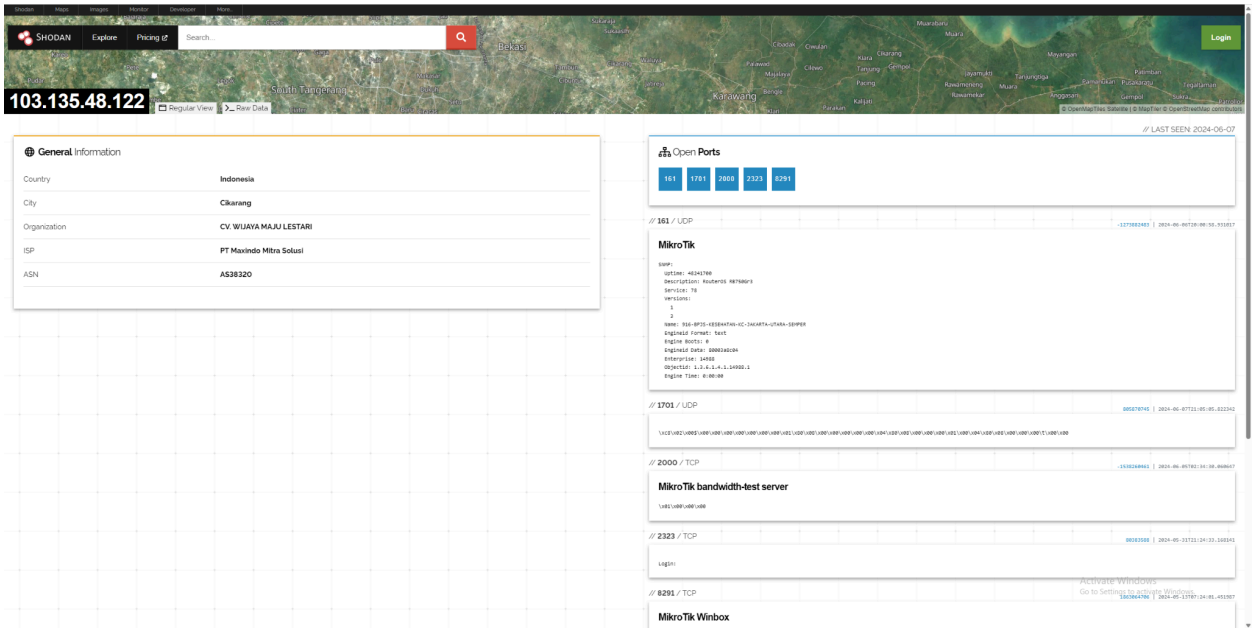

Informasi Umum

- **Negara:** Indonesia
- **Kota:** Cikarang
- **Organisasi:** CV. WIJAYA MAJU LESTARI
- **ISP:** PT Maxindo Mitra Solusi
- **ASN (Autonomous System Number):** AS38320

Port Terbuka

Informasi ini menunjukkan port-port jaringan yang terbuka pada sistem dengan rincian sebagai berikut:

Port 161 / UDP

- **Tanggal dan Waktu Pengamatan:** 2024-06-06T20:00:58.931017
- **Perangkat:** MikroTik
- **Protokol:** SNMP (Simple Network Management Protocol)
- **Informasi Tambahan:**
    - **Uptime:** 48241700 (waktu perangkat berjalan tanpa reboot dalam detik)
    - **Deskripsi:** RouterOS RB750Gr3 (model perangkat)
    - **Service:** 78 (jenis layanan yang berjalan)
    - **Versi SNMP:**
        - Versi 1
        - Versi 3
    - **Nama Perangkat:** 916-BPJS-KESEHATAN-KC-JAKARTA-UTARA-SEMPER

    - **Engine ID Format:** text
    - **Engine Boots:** 0 (jumlah restart dari engine SNMP)
    - **Engine ID Data:** 80003a8c04 (identifikasi unik untuk SNMP engine)
    - **Enterprise:** 14988 (ID perusahaan yang menggunakan perangkat)
    - **Object ID:** 1.3.6.1.4.1.14988.1 (identifikasi objek SNMP)
    - **Engine Time:** 0:00:00 (waktu sejak engine SNMP terakhir kali di-boot)

Port 1701 / UDP

- **Tanggal dan Waktu Pengamatan:** 2024-06-07T21:05:05.822342
- **Data Hex:** \xc8\x02\x00$\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x04\x80\x08\x00\x00\x00\x01\x00\x04\x80\x08\x00\x00\x00\t\x00\x00

Port 2000 / TCP

- **Tanggal dan Waktu Pengamatan:** 2024-06-05T02:34:30.060647
- **Perangkat:** MikroTik
- **Layanan:** Bandwidth-test server (server untuk menguji kecepatan bandwidth)
- **Data Hex:** \x01\x00\x00\x00

Port 2323 / TCP

- **Tanggal dan Waktu Pengamatan:** 2024-05-31T21:24:33.168141
- **Informasi:** Login prompt ditemukan, ini menunjukkan adanya layanan login yang terbuka.

Port 8291 / TCP

- **Tanggal dan Waktu Pengamatan:** 2024-05-13T07:24:01.451987
- **Perangkat:** MikroTik
- **Layanan:** MikroTik Winbox
- **Informasi Tambahan:**
    - **Versi Winbox:**
        - advtool.jg: 6.48.2
        - dhcp.jg: 6.48.2
        - hotspot.jg: 6.48.2
        - icons.png: 6.48.2
        - icons24.png:
        - icons32.png:
        - mpls.jg: 6.48.2
        - ppp.jg: 6.48.2
        - roteros.jg: 6.48.2
        - roting4.jg: 6.48.2

        - secure.jg: 6.48.2

Penjelasan dan Kemungkinan Celah Keamanan

1. **Port 161 (UDP) - SNMP:**
    - **Potensi Kerentanan:**
        - SNMPv1 dan SNMPv3 dapat memiliki kelemahan keamanan, terutama jika menggunakan versi yang tidak aman atau konfigurasi default yang lemah.
        - Mengakses informasi sensitif tentang perangkat jaringan.
    - **Langkah Mitigasi:**
        - Pastikan SNMP diatur menggunakan SNMPv3 dengan enkripsi dan otentikasi yang kuat.
        - Batasi akses SNMP hanya untuk IP tertentu.
2. **Port 1701 (UDP):**
    - **Potensi Kerentanan:**
        - Port ini biasanya digunakan untuk L2TP (Layer 2 Tunneling Protocol). Kerentanan bisa muncul jika layanan ini tidak dikonfigurasi dengan benar.
    - **Langkah Mitigasi:**
        - Pastikan layanan L2TP dikonfigurasi dengan otentikasi yang kuat dan hanya menerima koneksi dari sumber yang tepercaya.
3. **Port 2000 (TCP) - Bandwidth-test server:**
    - **Potensi Kerentanan:**
        - Bandwidth-test server bisa disalahgunakan untuk membebani jaringan.
    - **Langkah Mitigasi:**
        - Batasi akses ke layanan ini hanya untuk admin jaringan.
        - Pastikan layanan ini dinonaktifkan jika tidak digunakan.
4. **Port 2323 (TCP):**
    - **Potensi Kerentanan:**
        - Port ini sering digunakan sebagai alternatif untuk Telnet, yang tidak aman karena transmisi data dalam teks biasa.
    - **Langkah Mitigasi:**
        - Hindari penggunaan Telnet dan gunakan SSH sebagai gantinya.
        - Pastikan hanya pengguna yang sah yang memiliki akses ke layanan ini.
5. **Port 8291 (TCP) - MikroTik Winbox:**
    - **Potensi Kerentanan:**
        - Versi Winbox yang lama dapat memiliki kerentanan yang dikenal.
    - **Langkah Mitigasi:**
        - Pastikan perangkat menjalankan versi firmware terbaru.
        - Batasi akses ke Winbox hanya untuk alamat IP yang dipercaya.

bpjs-kesehatan.go.id Cross Site Scripting Vulnerability
Report ID: OBB-1051575

Security Researcher **iamDEAD**, a holder of 6 badges for responsible and coordinated disclosure, found Cross Site Scripting security vulnerability affecting **bpjs-kesehatan.go.id** website and its users.

Following the coordinated and responsible vulnerability disclosure guidelines of the **ISO 29147** standard, Open Bug Bounty has:

a. verified the vulnerability and confirmed its existence;
b. notified the website operator about its existence.

Affected Website:	bpjs-kesehatan.go.id
Open Bug Bounty Program:	Create your bounty program now. It's open and free.
Vulnerable Application:	Custom Code
Vulnerability Type:	XSS (Cross Site Scripting) / CWE-79
CVSSv3 Score:	6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]
Disclosure Standard:	Coordinated Disclosure based on ISO 29147 guidelines
Discovered and Reported by:	iamDEAD
Remediation Guide:	OWASP XSS Prevention Cheat Sheet
Export Vulnerability Data:	Bugzilla Vulnerability Data JIRA Vulnerability Data [Configuration] Mantis Vulnerability Data Splunk Vulnerability Data XML Vulnerability Data [XSD]

Vulnerable URL:

```
https://www.bpjs-kesehatan.go.id/bpjs/autodebit/detail/1/"><
svG onLoad=prompt(7)>
```

Research's Comment:

```
Just click on the vulnerable link and you will get a pop-up
of XSS. For more information mail me.
```

Mirror:

Click here to view the mirror

Laporan Kerentanan Keamanan

1. Informasi Umum

Situs Web yang Terkena:

- bpjs-kesehatan.go.id

Peneliti Keamanan:

- raviakp1004 (pemegang 7 lencana untuk pelaporan yang bertanggung jawab dan terkoordinasi)

Standar Pengungkapan:

- Pengungkapan Terkoordinasi berdasarkan panduan ISO 29147

2. Detail Kerentanan

Jenis Kerentanan:

- XSS (Cross Site Scripting) / CWE-79

Aplikasi yang Rentan:

- Custom Code

Skor CVSSv3:

- 6.1 [CVSS:3.0/AV
  /AC
  /PR
  /UI
  /S
  /C
  /I
  /A
  ]

Pemandu Remediasi:

- OWASP XSS Prevention Cheat Sheet

Skema Ekspor Data Kerentanan:

- Bugzilla Vulnerability Data
- JIRA Vulnerability Data
- Mantis Vulnerability Data
- Splunk Vulnerability Data
- XML Vulnerability Data [XSD]

3. Tindakan yang Telah Dilakukan

- **Verifikasi Kerentanan:**
  Kerentanan telah diverifikasi dan keberadaannya telah dikonfirmasi oleh Open Bug Bounty.
- **Pemberitahuan kepada Operator Situs:**
  Operator situs telah diberitahu tentang adanya kerentanan ini.

4. Tautan dan Program Bounty

- **Program Open Bug Bounty:**
  Buat program bounty Anda sekarang. Ini terbuka dan gratis.

5. URL dan Data yang Rentan

Vulnerable URL:

ruby
Copy code
```
https://www.bpjs-kesehatan.go.id/bpjs/post/read/2020/1602/Mudahkah-Badan-Usaha-BPJS-Kesehatan-Luncurkan-e-Dabu-Mobile/x"><svg onLoad=prompt(9)>
```

HTTP POST data:

ruby
Copy code
```
https://www.bpjs-kesehatan.go.id/bpjs/post/read/2020/1602/Mudahkah-Badan-Usaha-BPJS-Kesehatan-Luncurkan-e-Dabu-Mobile/x"><svg onLoad=prompt(9)>
```

Ringkasan

Kerentanan XSS ini memungkinkan penyerang untuk menyisipkan dan menjalankan skrip berbahaya di situs web bpjs-kesehatan.go.id, yang dapat digunakan untuk berbagai tujuan berbahaya seperti mencuri informasi pengguna atau menjalankan tindakan yang tidak sah atas

nama pengguna.

Langkah-Langkah Remediasi

1. **Identifikasi dan Validasi Input:**
    - Pastikan semua input pengguna divalidasi dan disanitasi dengan benar sebelum diproses.
2. **Menggunakan Karakter Escape:**
    - Terapkan karakter escape pada data yang akan ditampilkan di halaman web untuk mencegah injeksi skrip.
3. **Penerapan Kebijakan Keamanan Konten (Content Security Policy - CSP):**
    - Terapkan CSP untuk membatasi sumber daya yang dapat dimuat dan dijalankan oleh browser.
4. **Pembaruan dan Pemantauan:**
    - Selalu memperbarui aplikasi dan menerapkan patch keamanan yang tersedia.
    - Lakukan pemantauan secara berkala terhadap aktivitas mencurigakan di situs web.

Kesimpulan

Dengan mengikuti langkah-langkah remediasi yang disarankan oleh OWASP XSS Prevention Cheat Sheet, kerentanan ini dapat ditangani dengan baik, mengurangi risiko serangan XSS di masa depan dan meningkatkan keamanan situs web bpjs-kesehatan.go.id.

Pastikan untuk terus mengikuti praktik terbaik keamanan dan memperbarui aplikasi secara rutin untuk menjaga keamanan data dan pengguna.