LAPORAN

*DATA COLLECTION* DAN *VULNERABILITY ASSESMENT*

SITUS **UNSRI AC.ID** DAN **JAKARTA.GO.ID**


Nama : Devi Indra Meytri

NIM : 09031281520103

Kelas : Sistem Informasi Reguler 6A

Mata Kuliah : Manajemen Keamanan Informasi

JURUSAN SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA


MARET 2018

1. *Data Collection*

Setelah menentukan situs, maka dilakukan *data collection*. Untuk mengumpulkan data, dapat dilakukan 2 kegiatan yaitu foot printing dan scanning. Terdapat banyak *tools* yang dapat digunakan seperti whois, netcraft, buildwith untuk melakukan *foot printing* sedangkan *scanning* menggunakan aplikasi NMAP dan wireshark.

2. *Vulnerability Assesement*

*Vulnerability assesment* digunakan untuk mengetahui celah kekurangan dari teknologi yang digunakan oleh sebuah sistem. Website yang berisi informasi lengkap tentang vulnerability adalah cve.mitre.org. Terdapat banyak CVE yang tersedia.

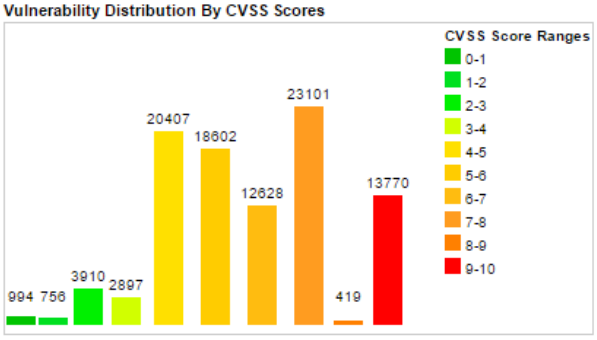
**Current CVSS Score Distribution For All Vulnerabilities**

**Distribution of all vulnerabilities by CVSS Scores**

| CVSS Score | Number Of Vulnerabilities | Percentage |
|---|---|---|
| 0-1 | 994 | 1.00 |
| 1-2 | 756 | 0.80 |
| 2-3 | 3910 | 4.00 |
| 3-4 | 2897 | 3.00 |
| 4-5 | 20407 | 20.90 |
| 5-6 | 18602 | 19.10 |
| 6-7 | 12628 | 13.00 |
| 7-8 | 23101 | 23.70 |
| 8-9 | 419 | 0.40 |
| 9-10 | 13770 | 14.10 |
| Total | 97484 | |

Weighted Average CVSS Score: **6.7**

**Vulnerability Distribution By CVSS Scores**




Sebuah CVE memiliki skor vulnerability yang ditemukan. Semakin tinggi skor CVSS mengindikasikan sistem tersebut lemah dan lebih mudah diserang.

**Vulnerability Details : CVE-2018-5703**

The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 allows attackers to cause a denial of service (slab out-of-bounds write) unspecified other impact via vectors involving TLS.

Publish Date : 2018-01-16 Last Update Date : 2018-02-15

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 10.0 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Denial Of Service |
| CWE ID | 787 |

**– Products Affected By CVE-2018-5703**

| # | Product Type | Vendor | Product | Version | Update | Edition | Language | |
|---|---|---|---|---|---|---|---|---|
| 1 | OS | Linux | Linux Kernel | 4.14.11 | | | | Version Details Vulnerabilities |

Gambar diatas menunjukkan skor CVE dengan ID CVE-2015-5703 adalah 10.0 disertai dengan deskripsi detil suatu *vulnerability*.

UNSRI.AC.ID

1) *Foot printing* dengan Netcraft.com

**Background**

| | | | |
|---|---|---|---|
| **Site title** | .:: Halaman Utama \| Universitas Sriwijaya - Indralaya, Sumatera Selatan | **Date first seen** | June 2000 |
| **Site rank** | | **Primary language** | Indonesian |
| **Description** | *Not Present* | | |
| **Keywords** | *Not Present* | | |
| **Netcraft Risk Rating [FAQ]** | 0/10 | | |

Pada gambar diatas dapat diketahui judul, waktu pertama kali website ada, bahasa yang digunakan, peringkat, deskripsi, kata kunci dan *Netcraft Risk Rating* yaitu level kemampuan situs lain untuk melakukan serangan yang belum ada pada database netcraft. Semakin rendah angka level maka semakin baik karena mengindikasikan semakin rendah resikonya. Banyak faktor yang mempengaruhi risk rating, diantaranya karena banyaknya phishing yang ada pada domain yang sama, nama hosting atau IP digunakan pada URL, riwayat hosting ISP, kota tempat hosting, dan top level domain yang dikenali situs *phishing* serta situsnya populer pada pencarian netcraft.

**Network**

| | | | |
|---|---|---|---|
| **Site** | http://unsri.ac.id | **Netblock Owner** | Universitas Sriwijaya |
| **Domain** | unsri.ac.id | **Nameserver** | ns1.unsri.ac.id |
| **IP address** | 103.241.4.11 | **DNS admin** | admin@unsri.ac.id |
| **IPv6 address** | 2001:df1:7000:0:0:0:0:a2 | **Reverse DNS** | ns4.unsri.ac.id |
| **Domain registrar** | pandi.or.id | **Nameserver organisation** | whois.pandi.or.id |
| **Organisation** | Universitas Sriwijaya, Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo, Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan, Palembang, 30138, Indonesia | **Hosting company** | unsri.ac.id |
| **Top Level Domain** | Indonesia (.ac.id) | **DNS Security Extensions** | *unknown* |
| **Hosting country** | ID | | |

Pada tabel network, terdapat informasi versi IP yaitu versi 6 yang dapat diambil untuk mengetahui *vulnerability* sistem. Mengetahui *vulnerability* dapat memanfaatkan CVE. Pada salah satu CVE yang ada tentang Ipv6 pada situs cve.mitre.org yang menyebutkan jika Ipv6 pada linux 4.14.11 dapat dilakukan serangan yang dapat mengakibatkan *denial of service* (pemberhentian layanan) dan lainnya.

## Hosting History

| Netblock owner | IP address | OS | Web server | Last seen |
|---|---|---|---|---|
| Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia | 103.241.4.11 | Linux | nginx | 6-Mar-2018 |
| Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia | 103.241.4.11 | Linux | nginx/1.1.19 | 24-Apr-2016 |
| Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Ilir Sumatera Selatan 30662, Indonesia | 103.241.4.11 | Linux | Apache | 3-Mar-2016 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache | 2-Nov-2013 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache/2.2.22 Ubuntu | 25-Nov-2012 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache | 6-Sep-2012 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache/2.2.3 CentOS | 6-Aug-2012 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | unknown | 1-Mar-2011 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache/2.2.3 CentOS | 26-Feb-2011 |
| PT Telkom Indonesias customer. | 222.124.194.11 | Linux | Apache/2.2.8 Fedora | 23-Mar-2009 |

Tabel riwayat hosting situs unsri.ac.id menampilkan informasi bahwa telah terjadi perubahan tempat hosting yaitu PT Telkom Indonesia Customer pada tahun 2009 – 2013 dengan OS Linux dan webserver Apache. Setelah itu berganti hosting Unsri mulai Maret 2016 dengan OS Linux dan Web server nginx.

## Vulnerability Details : CVE-2017-7529

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

Publish Date : 2017-07-13 Last Update Date : 2018-01-04

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

### - CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 5.0 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Overflow Obtain Information |
| CWE ID | 190 |

CVE-2017-7529 dengan skor CVE 5.0, Nginx versi 0.5.6 hingga 1.13.2 berpotensi terdapat triger informasi sensitif sehingga terjadi kebocoran dengan dengan request dari orang yang memiliki keahlian khusus. Tidak ada autentikasi untuk dapat melakukan exploit, namum sangat sedikit seklai orang yang memiliki pengetahuan dan skill untuk melakukan exploit . Gangguan yang terjadi berupa terbongkarnya informasi namum tidak berimbas pada availability dan integritas sistem.

**HTTP Compression**

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| **Gzip Content Encoding** | Gzip HTTP Compression protocol | www.virustotal.com, www.bloomberg.com, www.fanfiction.net |

## Vulnerability Details : CVE-2002-2395

InterScan VirusWall 3.52 for Windows allows remote attackers to bypass virus protection and possibly execute arbitrary code via HTTP 1.1 gzip content encoding.

Publish Date : 2002-12-31 Last Update Date : 2008-09-05

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

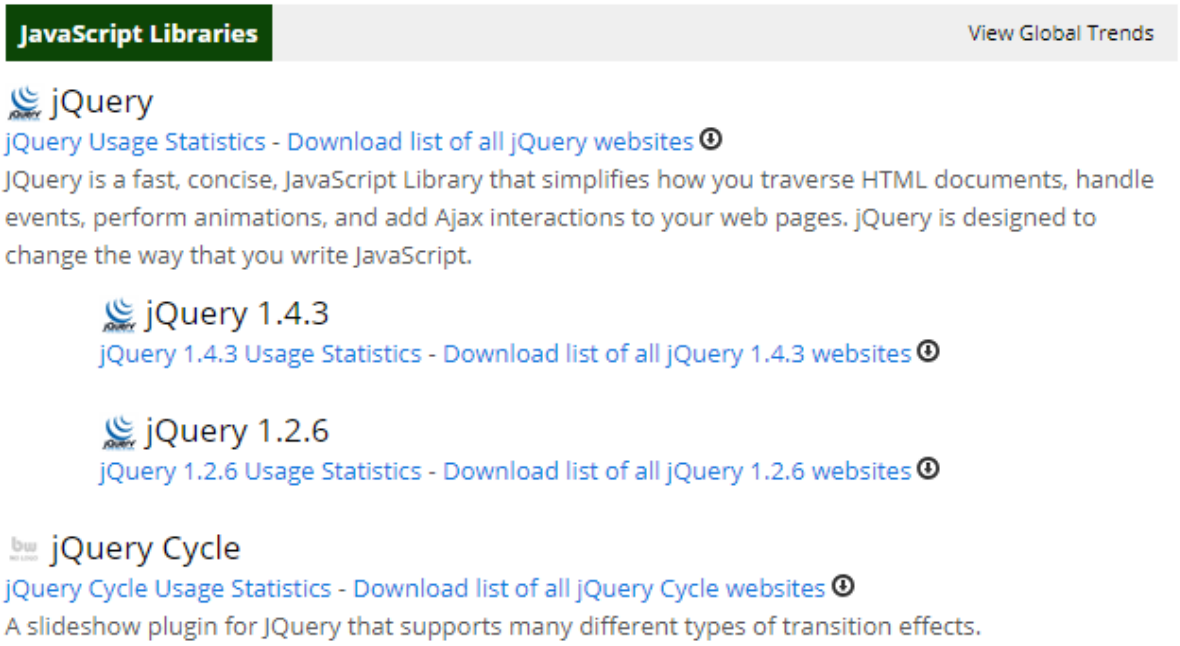
Search Twitter Search YouTube Search Google

### - CVSS Scores & Vulnerability Types

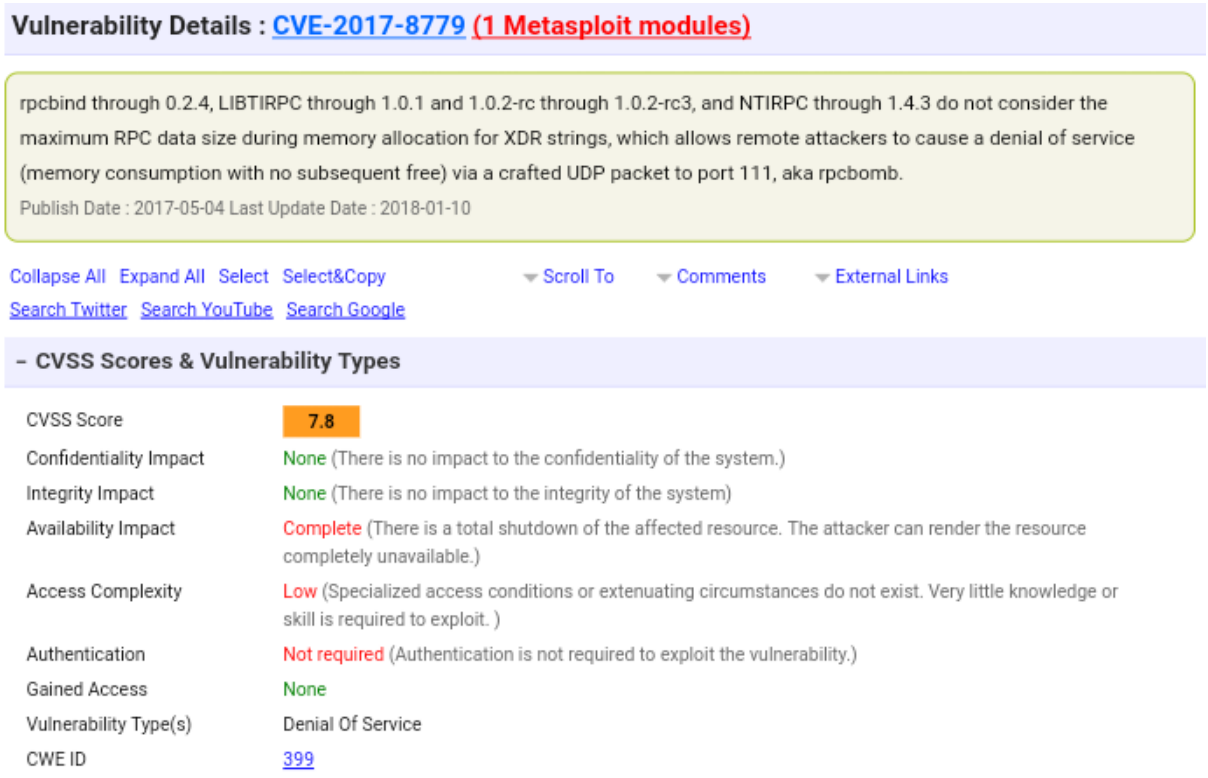
| | |
|---|---|
| CVSS Score | 5.0 |
| Confidentiality Impact | None (There is no impact to the confidentiality of the system.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code Bypass a restriction or similar |
| CWE ID | 264 |

Terdapat satu CVE dengan ID CVE-2002-2395 dan skor 5.0 tentang Gzip content encoding yang menyatakan bahwa dengan menggunakan InterScan VirusWall 3.52 pada Windows penyerang dapat melewati proteksi virus dan memungkinkan mengubag kode dengan menggunakan HTTP 1.1 gzip content encoding. Tidak berimbas pada kerahasiaan sistem, memungkinkan adanya modifikasi informasi atau file namum lefek yang ditimbulkan terbatas, dan tidak berpengaruh pada availability sistem.

2) *Foot printing* dengan Buildwith.com

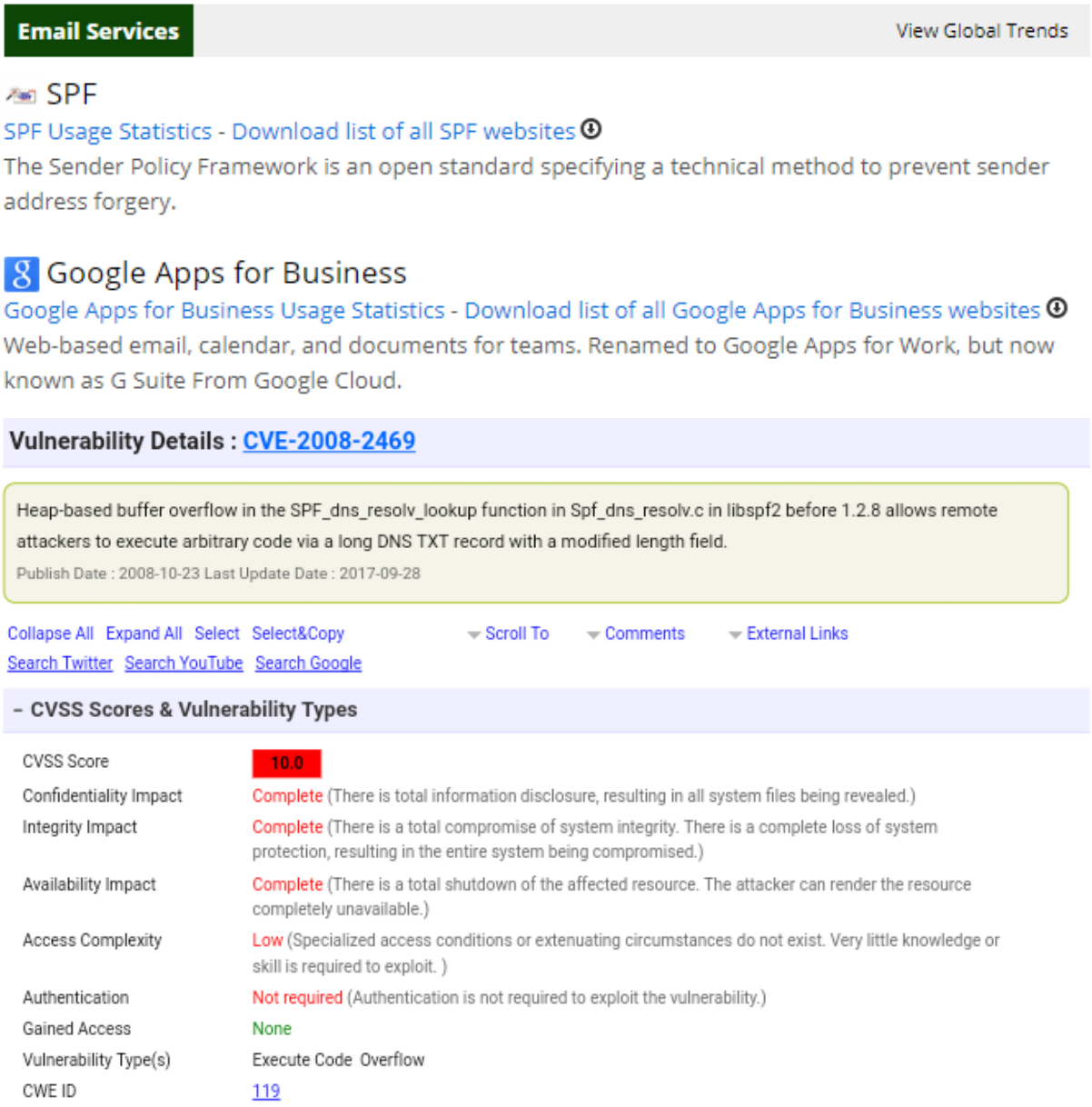



Pada builtwith.com diketahui jika unsri.ac.id menggunakan librari Javascript jQuery 1.4.3.

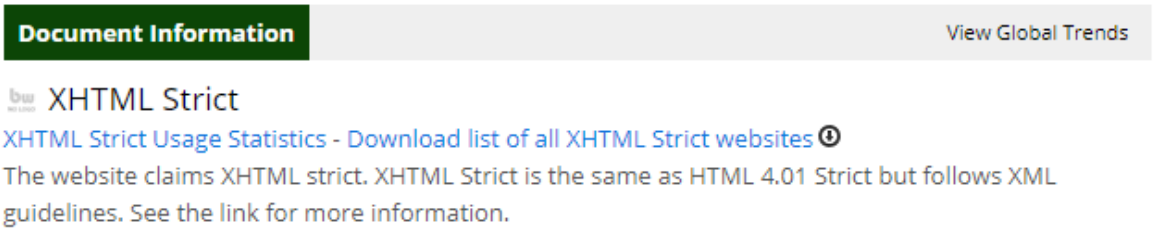


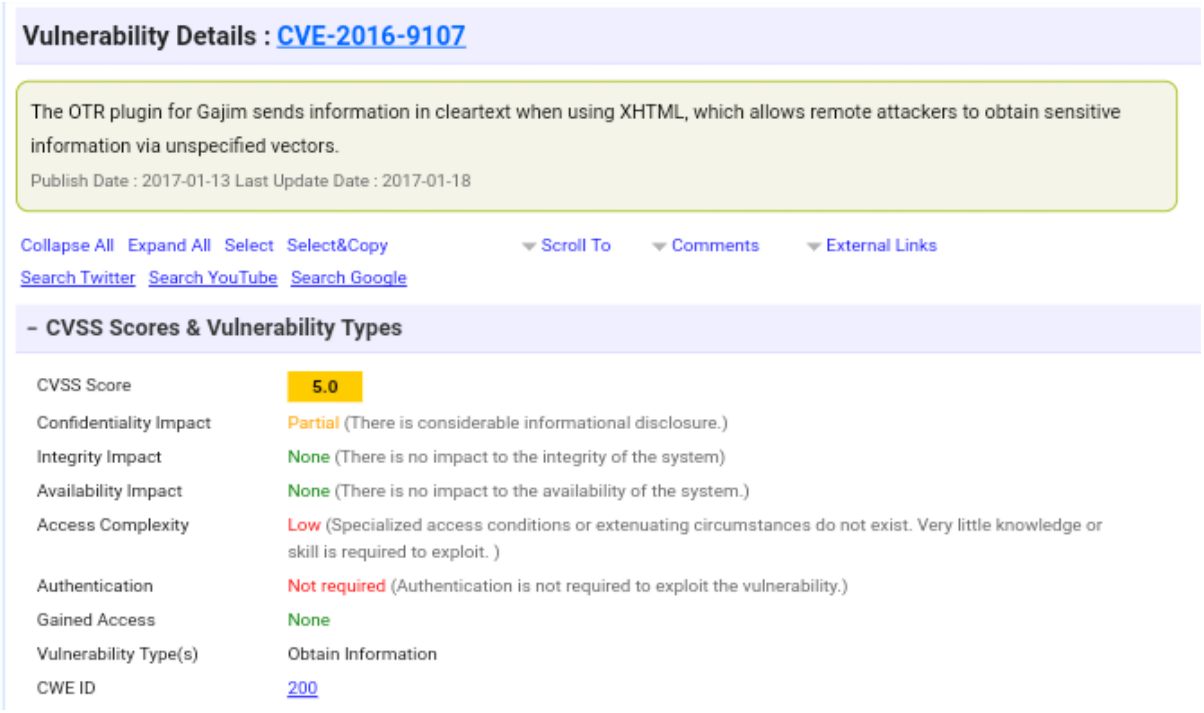

CVE-2017-8779 dengan skor 7.8 menyebutkan bahwa dapat menyebabkan denial pada layanan sehingga memori digunakan tanpa ada yang dibebaskan dengan mengirimkan paket UDP pada port 111. Hal ini dapat menyebabkan kematian total resource dan penyerang (attacker) dapat membuat resorce tidak tersedia sama sekali.


CVE-2018-0101memiliki skor 10.0 dapat menyebabkan informasi terbongkar secara total yang membuat seluruh file dapat dicuri, berimbas pada integritas sistem, resource sistem dapat mati total




CVE-2008-2469 dengan skor 10.0 dapat mengakibatkan seluruh informasi pada sistem terbuka dan dapat dicuri, dimana attacker dapat mengubah kode dengan sebuah baris DNS TXT yang panjang dengan modifikasi panjang kolom.





## Vulnerability Details : CVE-2016-9107

The OTR plugin for Gajim sends information in cleartext when using XHTML, which allows remote attackers to obtain sensitive information via unspecified vectors.

Publish Date : 2017-01-13 Last Update Date : 2017-01-18

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

### - CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 5.0 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | None (There is no impact to the integrity of the system) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Obtain Information |
| CWE ID | 200 |

CVE-2016-9107 dengan skor 5.0, dapat terjadi pencurian informasi pada penggunaan plugin OTR untuk mengirim informasi dengan bentuk teks yang jelas menggunakan XHTML memungkinkan attacker dapat mencuri informasi melalui posisi yang tidak bisa ditentukan. Namu hal ini tidak mempengaruhi integritas dan availability sistem.

JAKARTA.GO.ID

1) *Foot printing* dengan Netcraft.com

## Background

| | | | |
|---|---|---|---|
| **Site title** | *Not Present* | **Date first seen** | September 1998 |
| **Site rank** | | **Primary language** | English |
| **Description** | *Not Present* | | |
| **Keywords** | *Not Present* | | |
| **Netcraft Risk Rating [FAQ]** | 7/10 | | |

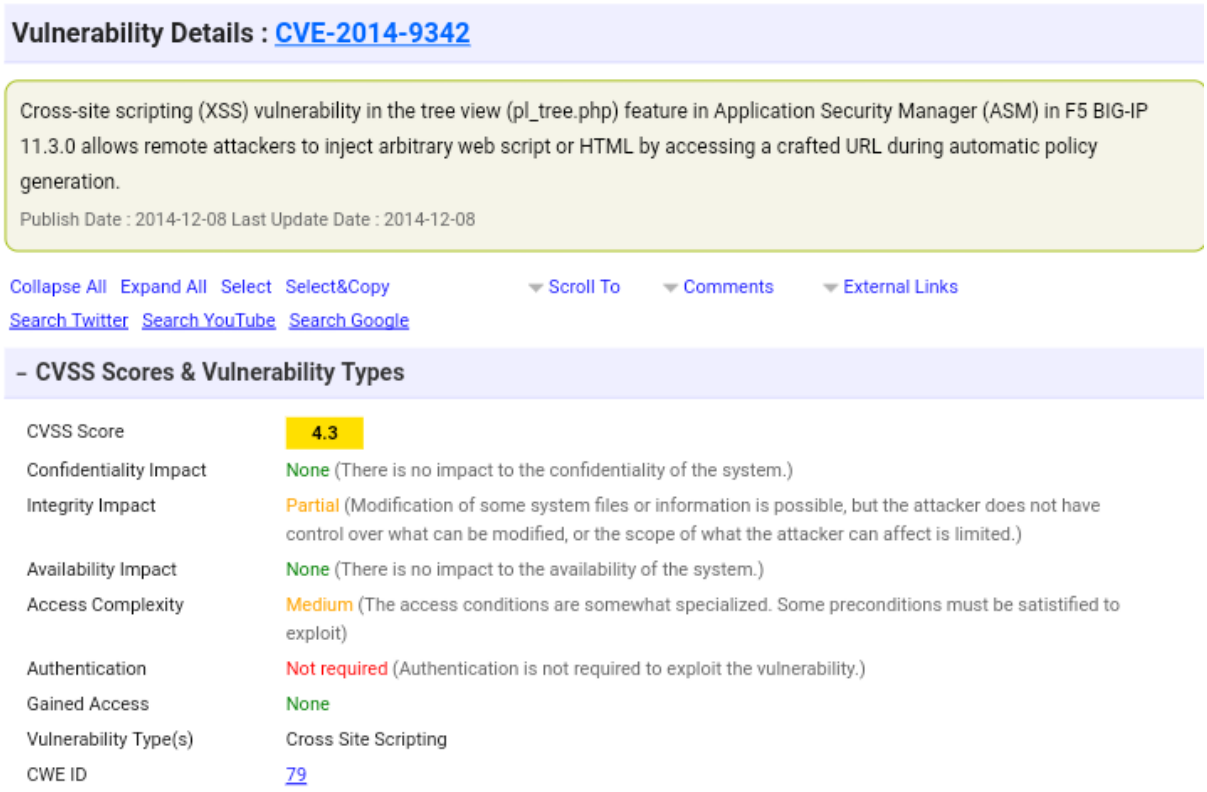
## Network

| | | | |
|---|---|---|---|
| **Site** | http://jakarta.go.id | **Netblock Owner** | Diskominfo DKI Jakarta |
| **Domain** | jakarta.go.id | **Nameserver** | ns1.jakarta.go.id |
| **IP address** | 103.209.7.21 | **DNS admin** | root@jakarta.go.id |
| **IPv6 address** | *Not Present* | **Reverse DNS** | *unknown* |
| **Domain registrar** | *unknown* | **Nameserver organisation** | *unknown* |
| **Organisation** | *unknown* | **Hosting company** | *unknown* |
| **Top Level Domain** | Indonesia (.go.id) | **DNS Security Extensions** | Enabled |
| **Hosting country** | ID | | |

Netcraft risk rating situs jakarta.go.id adalah 7, yang berarti situs ini beresiko mengalami serangan dan banyak dicari pada situs netcraft.

## Hosting History

| Netblock owner | IP address | OS | Web server | Last seen Refresh |
|---|---|---|---|---|
| Diskominfo DKI Jakarta Government / Direct Member IDNIC Jl. Jl. Medan Merdeka Selatan No. 8-9 Jakarta Pusat, Indonesia | 103.209.7.21 | unknown | BigIP | 6-Mar-2018 |
| Diskominfo DKI Jakarta Government / Direct Member IDNIC Jl. Jl. Medan Merdeka Selatan No. 8-9 Jakarta Pusat, Indonesia | 103.209.7.21 | unknown | unknown | 28-Nov-2016 |
| PT Telkom Indonesias customer. | 118.97.66.21 | unknown | unknown | 28-Sep-2016 |
| PT Telkom Indonesias customer. | 118.97.66.7 | Linux | Apache/2.2.3 Red Hat | 16-Dec-2014 |
| PT Telkom Indonesias customer. | 118.97.66.7 | Linux | unknown | 10-Nov-2012 |
| PT. Platinum Network Indonesia Internet Service Provider Jakarta | 114.31.241.7 | Linux | unknown | 16-Apr-2010 |
| ISP PT. Sejuta Jaring Global JALAN RAYA BULUNGAN NO.1 JAKARTA SELATAN | 202.57.16.58 | - | Apache/1.3.23 Unix Red-Hat/Linux mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 | 28-Mar-2005 |
| ISP PT. Sejuta Jaring Global JALAN RAYA BULUNGAN NO.1 JAKARTA SELATAN | 202.57.16.58 | Linux | unknown | 27-Mar-2005 |
| ISP PT. Sejuta Jaring Global JALAN RAYA BULUNGAN NO.1 JAKARTA SELATAN | 202.57.16.58 | Linux | Apache/1.3.23 Unix Red-Hat/Linux mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 | 4-Jun-2004 |
| ISP PT. Sejuta Jaring Global JALAN RAYA BULUNGAN NO.1 JAKARTA SELATAN | 202.57.16.58 | Linux | unknown | 3-Jun-2004 |



**Vulnerability Details : CVE-2014-9342**

Cross-site scripting (XSS) vulnerability in the tree view (pl_tree.php) feature in Application Security Manager (ASM) in F5 BIG-IP 11.3.0 allows remote attackers to inject arbitrary web script or HTML by accessing a crafted URL during automatic policy generation.

Publish Date : 2014-12-08 Last Update Date : 2014-12-08

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

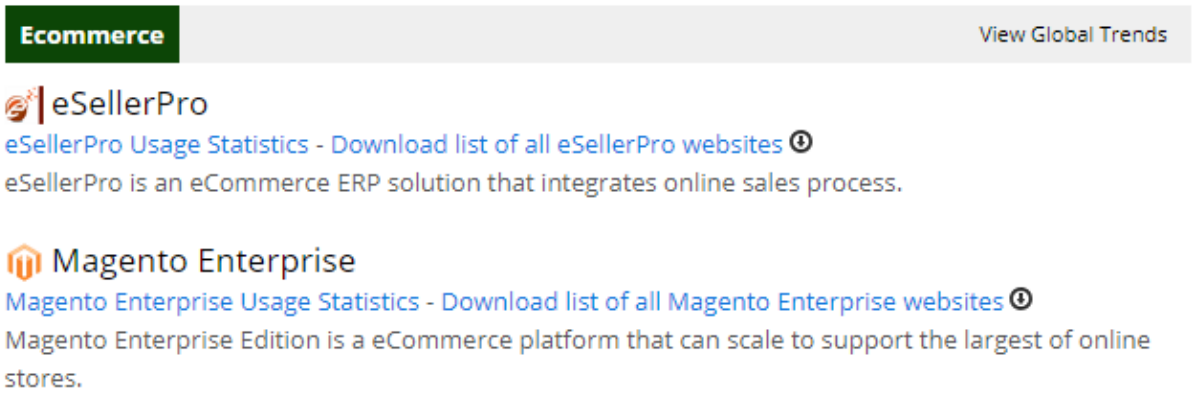
Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 4.3 |
| Confidentiality Impact | None (There is no impact to the confidentiality of the system.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | None (There is no impact to the availability of the system.) |
| Access Complexity | Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Cross Site Scripting |
| CWE ID | 79 |

CVE-2014-9342 skor 4.3 BigIP Cross-site scripting (XSS) vulnerability pada fitur three view (pl.three.php) di Application Security Manager (ASM) BIG-IP 11.3.0 memungkinkan attacker dapat memasukkan perubahan skri website atau HTML dengan mengakses URL pada generasi peraturan otomatis. Attacker dapat mengubah file namun lingkupnya terbatas.

2) *Foot printing* dengan Builtwith.com



**Ecommerce** View Global Trends

eSellerPro

eSellerPro Usage Statistics - Download list of all eSellerPro websites

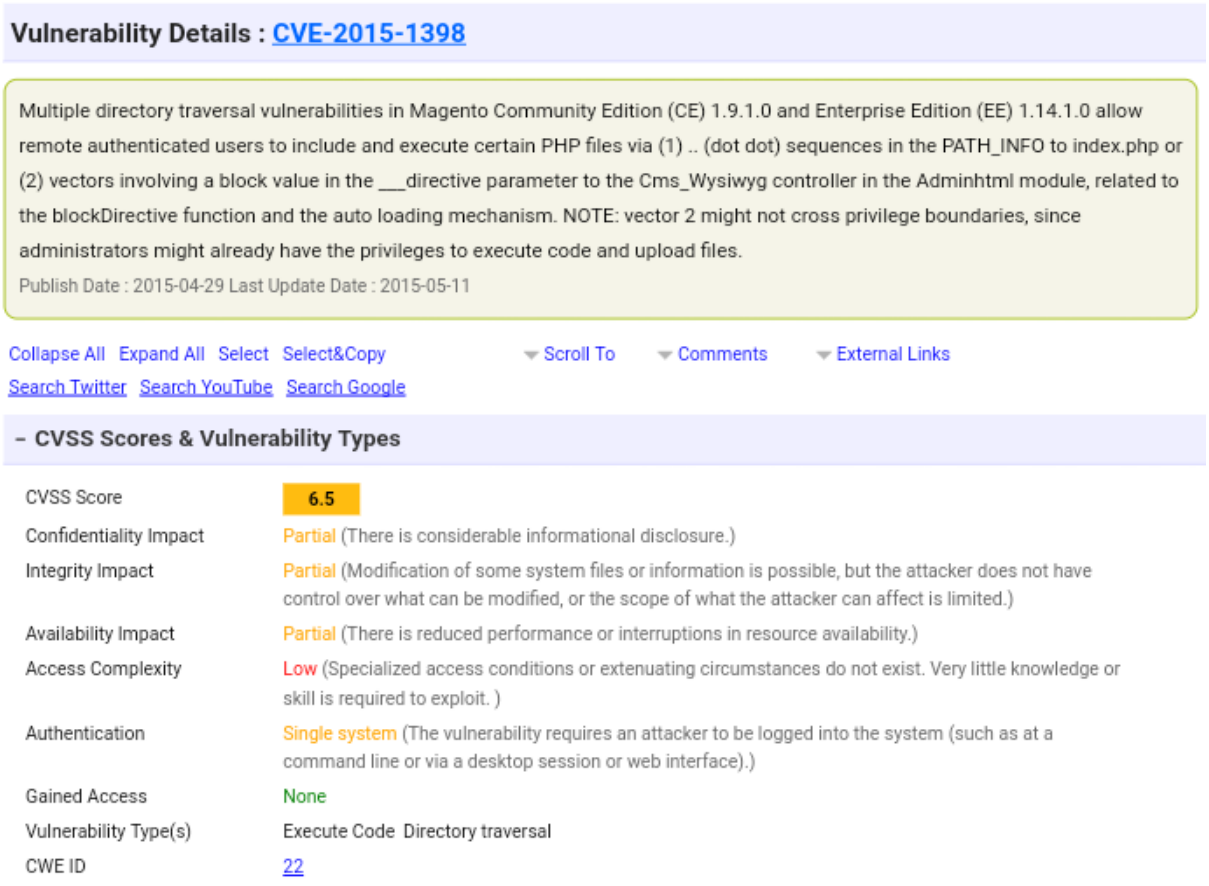
eSellerPro is an eCommerce ERP solution that integrates online sales process.

Magento Enterprise

Magento Enterprise Usage Statistics - Download list of all Magento Enterprise websites

Magento Enterprise Edition is a eCommerce platform that can scale to support the largest of online stores.

Magento CVE-2016-2212 skor 5.0 dapat terjadi pencurian informasi dengan menggunakan order_id pada sebuah JSON object pada parameter data di sebuah permintaan RSS ke index.php/rss/order/status.



**Vulnerability Details : CVE-2015-1398**

Multiple directory traversal vulnerabilities in Magento Community Edition (CE) 1.9.1.0 and Enterprise Edition (EE) 1.14.1.0 allow remote authenticated users to include and execute certain PHP files via (1) .. (dot dot) sequences in the PATH_INFO to index.php or (2) vectors involving a block value in the ___directive parameter to the Cms_Wysiwyg controller in the Adminhtml module, related to the blockDirective function and the auto loading mechanism. NOTE: vector 2 might not cross privilege boundaries, since administrators might already have the privileges to execute code and upload files.

Publish Date : 2015-04-29 Last Update Date : 2015-05-11

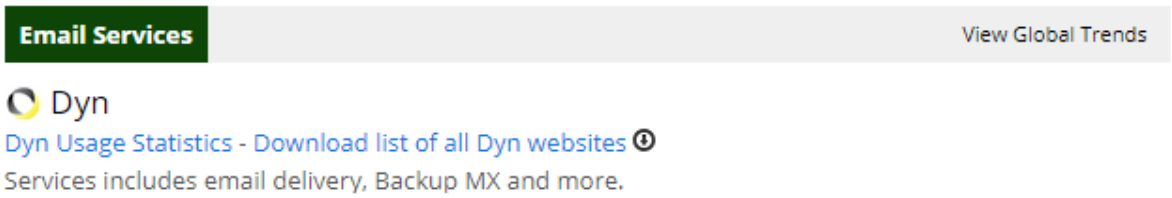
Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

**– CVSS Scores & Vulnerability Types**

| | |
|---|---|
| CVSS Score | 6.5 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | Partial (There is reduced performance or interruptions in resource availability.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code Directory traversal |
| CWE ID | 22 |

Sedangkan pada CVE-2015-1398 dengan skor 6.5, Magento versi 1.9.1.0 dan 1.14.1.0 memungkinkan atentikasi user termasuk eksekusi file PHP pada PATH_INFO ke index.php atau mengontrol modul Adminhtml dan automatis loading mekasisme namum dapat dilakukan setelah administrator memberi kode akses dan mengupload file. Hal ini dapat mengurangi performa atau interupsi ketersediaan resource. Vulnerability ini mengharuskan attacker masuk ke sistem seperti pada command line, sesi pada desktop atau tampilan website.



**Email Services** View Global Trends

Dyn

Dyn Usage Statistics - Download list of all Dyn websites

Services includes email delivery, Backup MX and more.

## Vulnerability Details : CVE-2010-4400 (2 public exploits)

SQL injection vulnerability in _rights.php in DynPG CMS 4.2.0 allows remote attackers to execute arbitrary SQL commands via the giveRights_UserId parameter.

Publish Date : 2010-12-06 Last Update Date : 2010-12-20

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

### - CVSS Scores & Vulnerability Types

| | |
|---|---|
| CVSS Score | 7.5 |
| Confidentiality Impact | Partial (There is considerable informational disclosure.) |
| Integrity Impact | Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.) |
| Availability Impact | Partial (There is reduced performance or interruptions in resource availability.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Execute Code Sql Injection |
| CWE ID | 89 |

CVE-2010-4400 dengan skor 7.5 dengan SQL injection pada _rights.php pada DynPG CMS 4.2.0 memungkinkan attacker mengubah SQL dengan parameter giveRights_UserId. Sehingga mengakibatkan perubahan file atau informasi dan mengurangi performa sistem.