LAPORAN
MANAJEMEN KEAMANAN INFORMASI

OLEH :

TRIANA LIONI PUTRI **09031281520089**

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2018

1. Website Sulutprov.go.id

- Data website sulutprov.go.id

Network

Site	http://sulutprov.go.id	**Netblock Owner**	PT Infotek Global Network
Domain	sulutprov.go.id	**Nameserver**	ns1.dreamhost.com
IP address	103.206.169.133	**DNS admin**	hostmaster@dreamhost.com
IPv6 address	*Not Present*	**Reverse DNS**	webhosting.infotek.net.id
Domain registrar	*unknown*	**Nameserver organisation**	whois.dreamhost.com
Organisation	*unknown*	**Hosting company**	infotek.net.id
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	Enabled
Hosting country	ID		

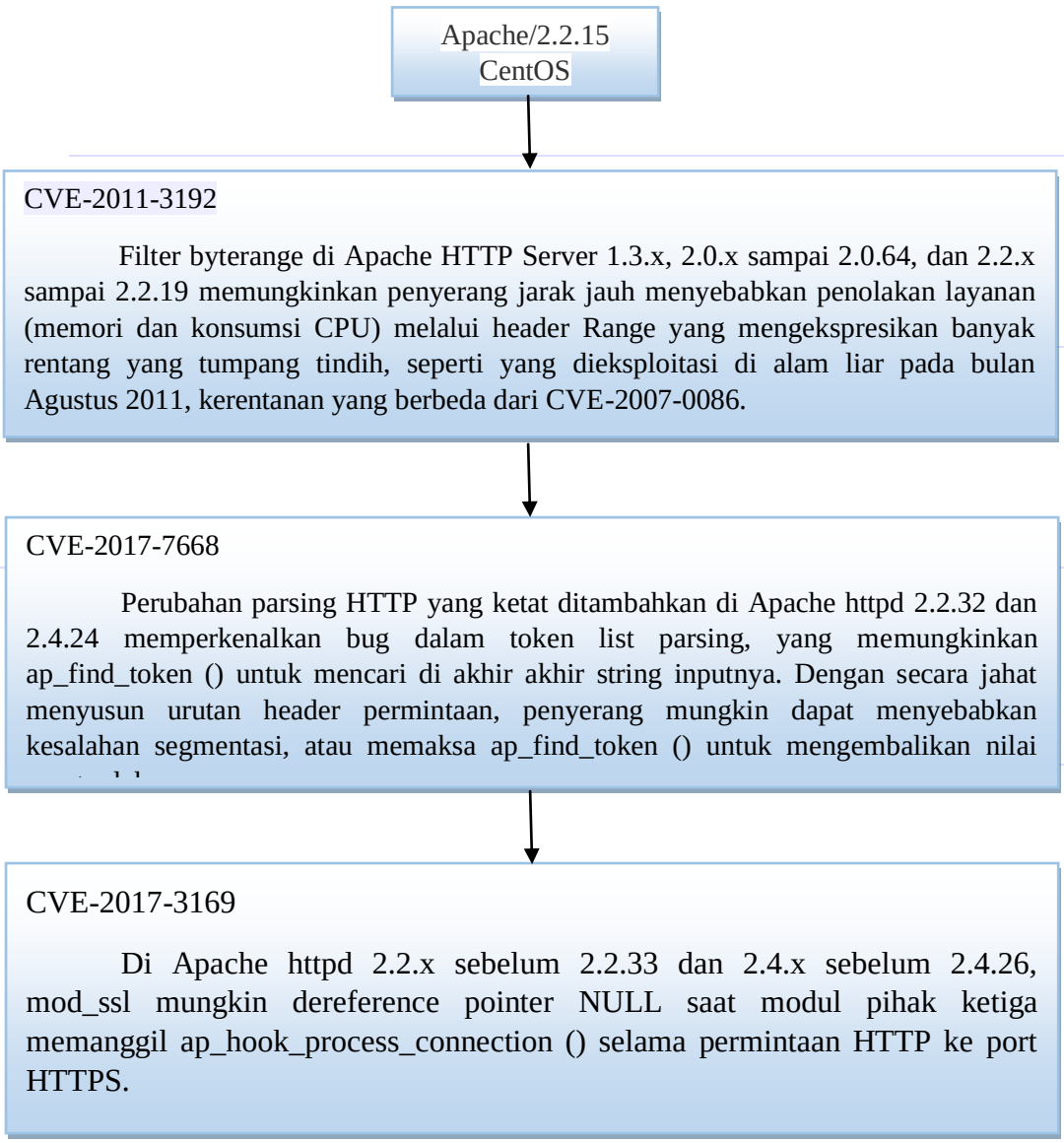
Domain Name:SULUTPROV.GO.ID
Created On:16-Feb-2011 13:35:21 UTC
Last Updated On:05-Apr-2017 00:07:27 UTC
Expiration Date:18-Feb-2019 23:59:59 UTC
Status:ok
Status:autoRenewPeriod
Registrant ID:sulawe-86506
Registrant Name:Sulawesi Utara
Registrant Organization:Sulawesi Utara
Registrant Street1:Jalan. 17 Agustus nomor 69
Registrant City:Manado
Registrant State/Province:Sulawesi Utara
Registrant Postal Code:95119
Registrant Country:ID
Registrant Phone:+62.431867052
Registrant Email: j_renbet@yahoo.com

- History hosting

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Infotek Global Network Internet Service Provider Hotel Gran Puri Lt.5 Jl. Sam Ratulangi No.458 Manado, Sulawesi Utara, 95116	103.206.169.133	Linux	Apache/2.2.15 CentOS	30-Aug-2016
SimplerCloud Pte Ltd Cloud Servers	103.25.202.42	Linux	Apache/2.2.15 CentOS	17-Feb-2016

- Vulnerabilities Web Server



- Vulnerabilities OS

Linux

CVE-2018-5703

Fungsi tcp_v6_syn_recv_sock di net / ipv6 / tcp_ipv6.c di kernel Linux melalui 4.14.11 memungkinkan penyerang untuk menyebabkan penolakan layanan (lemparan di luar batas penulisan) atau mungkin memiliki dampak lain yang tidak ditentukan melalui vektor yang melibatkan TLS.

CVE-2017-18017

Fungsi tcpmss_mangle_packet di net / netfilter / xt_TCPMSS.c di kernel Linux sebelum 4.11, dan 4.9.x sebelum 4.9.36, memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (penggunaan setelah bebas dan korupsi memori) atau mungkin tidak ditentukan Dampak lainnya dengan memanfaatkan kehadiran xt_TCPMSS dalam tindakan iptables.

CVE-2017-13715

Fungsi __skb_flow_dissect di net / core / flow_dissector.c di kernel Linux sebelum 4.3 tidak memastikan bahwa n_proto, ip_proto, dan thoff diinisialisasi, yang memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (system crash) atau mungkin mengeksekusi kode yang sewenang-wenang melalui paket MPLS tunggal yang dibuat.

-

2. Website Citilink.co.id

- Data website citilink.co.id

Network

Site	http://citilink.co.id	**Netblock Owner**	Microsoft Corporation
Domain	citilink.co.id	**Nameserver**	ns1.citilink.co.id
IP address	23.101.19.173	**DNS admin**	hostmaster@citilink.co.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pandi.or.id
Organisation	PT. Garuda Indonesia Persero Tbk., 1st fl. GMF Management Building Garuda City, Soekarno - Hatta International Airport, Tangerang, 19120, Indonesia	**Hosting company**	Microsoft - South East Asia (Sinapore) datacenter
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	sg		

Domain Name:CITILINK.CO.ID
Created On:16-Jan-2007 13:32:56 UTC
Last Updated On:09-Sep-2017 04:42:08 UTC
Expiration Date:01-Sep-2019 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:achmad-65677
Registrant Name:Achmad Royhan
Registrant Organization:PT. Garuda Indonesia Persero Tbk.
Registrant Street1:1st fl. GMF Management Building Garuda City
Registrant Street2:Soekarno - Hatta International Airport
Registrant City:Tangerang
Registrant State/Province:Banten
Registrant Postal Code:19120
Registrant Country:ID
Registrant Phone:+62.2155915609
Registrant Email:royhan@citilink.co.id

- Hosting history

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Microsoft Corporation One Microsoft Way Redmond WA US 98052	23.101.19.173	Windows Server 2012	Microsoft-IIS/8.5	19-Jun-2016
KASKUS Cloud Computing Jakarta	112.78.176.58	Linux	nginx/0.7.65	1-Aug-2014
PT Graha Multimedia Nusantara Corporate / Direct Member IDNIC Rasuna Office Park III, UO-11 Kompleks Rasuna Epicentrum Jl. HR Rasuna Said, Kuningan Jakarta Selatan, 12960	203.153.120.132	Windows Server 2003	Microsoft-IIS/6.0	3-Mar-2011

- Vulnerabilities Web Server

Microsoft-IIS/8.5

CVE-2014-4078

Fitur Keamanan IP di Microsoft Internet Information Services (IIS) 8.0 dan 8.5 tidak memproses dengan benar wildcard mengizinkan dan menolak aturan untuk domain dalam daftar "Alamat IP dan Pembatasan Domain", yang mempermudah penyerang jarak jauh untuk melewati aturan yang ditetapkan. via permintaan HTTP, alias "IIS Security Feature Bypass Vulnerability."

nginx/0.7.65

CVE-2010-2263

nginx 0.8 sebelum 0.8.40 dan 0.7 sebelum 0.7.66, saat berjalan di Windows, memungkinkan penyerang jarak jauh mendapatkan kode sumber atau konten yang tidak dipasteile dari file sewenang-wenang di bawah akar dokumen web dengan menambahkan :: $ DATA ke URI.

Microsoft-IIS/6.0

CVE-2017-7269

Buffer overflow dalam fungsi ScStoragePathFromUrl di layanan WebDAV di Internet Information Services (IIS) 6.0 di Microsoft Windows Server 2003 R2 memungkinkan penyerang jarak jauh untuk mengeksekusi kode sewenang-wenang melalui sebuah header panjang yang dimulai dengan "If: <http: //" dalam permintaan PROPFIND , seperti yang dieksploitasi di alam liar pada bulan Juli atau Agustus 2016.

- Vulnerabilities OS

Windows Server 2012

CVE-2015-6108

Perpustakaan font Windows di Microsoft Windows Vista SP2; Windows Server 2008 SP2 dan R2 SP1; Windows 7 SP1; Windows 8; Windows 8.1; Windows Server 2012 Gold dan R2; Windows RT Gold dan 8.1; Kantor 2007 SP3; Kantor 2010 SP2; Penampil kata; .NET Framework 3.0 SP2, 3.5, 3.5.1, 4, 4.5, 4.5.1, 4.5.2, dan 4.6; Skype untuk Bisnis 2016; Lync 2010; Lync 2013 SP1; Konsol Live Meeting 2007; dan Silverlight 5 memungkinkan penyerang remote untuk mengeksekusi kode sewenang-wenang melalui font tertanam yang dibuat, alias "Graphics Memory Corruption Vulnerability."

Linux

CVE-2018-5703

Fungsi tcp_v6_syn_recv_sock di net / ipv6 / tcp_ipv6.c di kernel Linux melalui 4.14.11 memungkinkan penyerang untuk menyebabkan penolakan layanan (lemparan di luar batas penulisan) atau mungkin memiliki dampak lain yang tidak ditentukan melalui vektor yang melibatkan TLS.

Windows Server 2003

CVE-2017-8461

Windows RPC dengan Routing dan Remote Access yang diaktifkan pada Windows XP dan Windows Server 2003 memungkinkan penyerang untuk mengeksekusi kode pada server RPC yang ditargetkan yang memiliki Routing and Remote Access yang diaktifkan melalui aplikasi yang dibuat secara khusus, alias "Windows RPC Remote Code Execution Vulnerability."