LAPORAN

TUGAS MANAJEMEN KEAMANAN INFORMASI

OLEH :

Nama	**:**	**NURANI**
NIM	**:**	**09031181520123**
Kelas	**:**	**SI Regular 6A**
Dosen Pembimbing	**:**	**Deris Stiawan, M.T., Ph.D.**

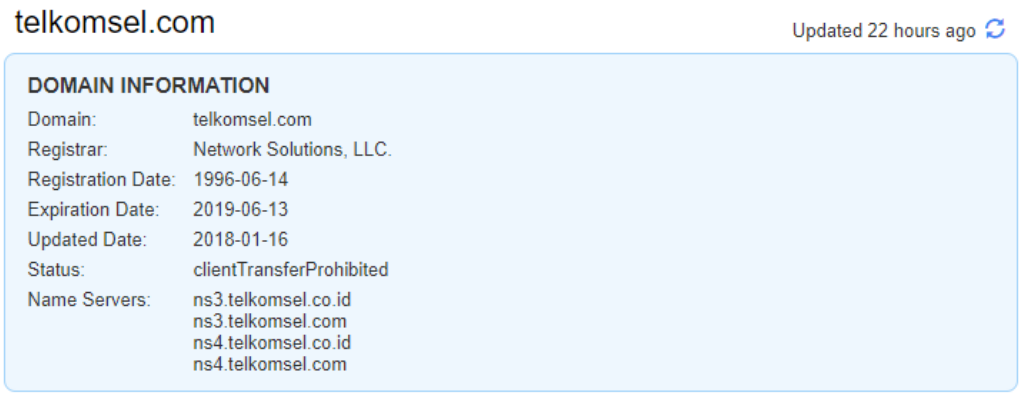
SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2018

Target : telkomsel.com

Data collection :



telkomsel.com

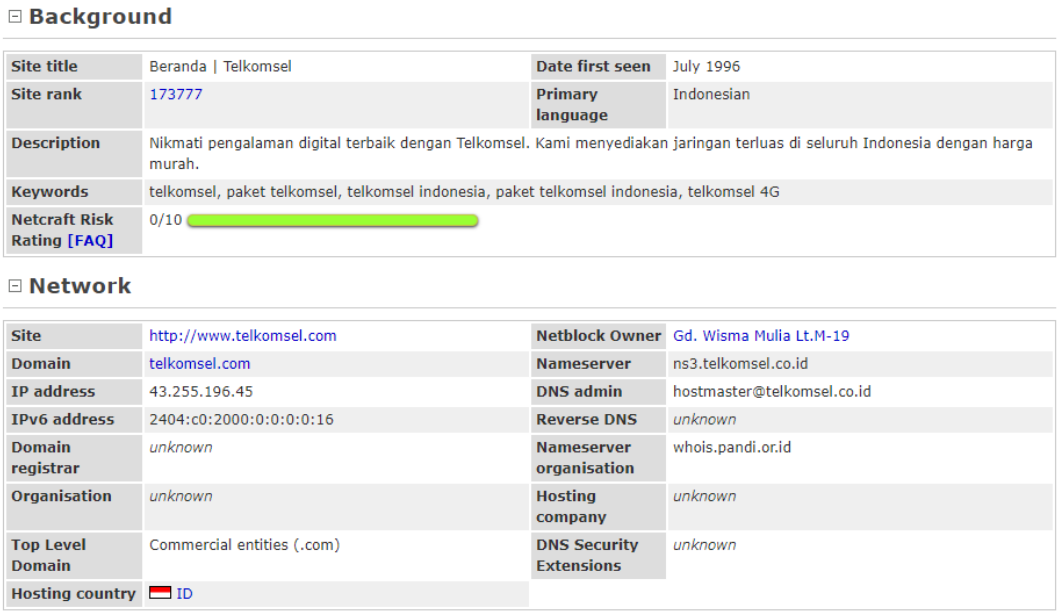
Updated 22 hours ago

DOMAIN INFORMATION

Domain:	telkomsel.com
Registrar:	Network Solutions, LLC.
Registration Date:	1996-06-14
Expiration Date:	2019-06-13
Updated Date:	2018-01-16
Status:	clientTransferProhibited
Name Servers:	ns3.telkomsel.co.id ns3.telkomsel.com ns4.telkomsel.co.id ns4.telkomsel.com

Gambar 1

Domain informasi yang terlihat pada gambar 1 didapat dari hasil track pada tools whois.com



Background

Site title	Beranda | Telkomsel	**Date first seen**	July 1996
Site rank	173777	**Primary language**	Indonesian
Description	Nikmati pengalaman digital terbaik dengan Telkomsel. Kami menyediakan jaringan terluas di seluruh Indonesia dengan harga murah.		
Keywords	telkomsel, paket telkomsel, telkomsel indonesia, paket telkomsel indonesia, telkomsel 4G		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.telkomsel.com	**Netblock Owner**	Gd. Wisma Mulia Lt.M-19
Domain	telkomsel.com	**Nameserver**	ns3.telkomsel.co.id
IP address	43.255.196.45	**DNS admin**	hostmaster@telkomsel.co.id
IPv6 address	2404:c0:2000:0:0:0:0:16	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	whois.pandi.or.id
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Gambar 2

Sedangkan pada gambar 2, didapat dari hasil track pada tools netcraft.com yang menampilkan informasi background dan network.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Gd. Wisma Mulia Lt.M-19	43.255.196.45	Citrix Netscaler	unknown	6-Mar-2018
Gd. Wisma Mulia Lt.M-19	103.239.188.20	Citrix Netscaler	nginx	25-Aug-2017
Gd. Wisma Mulia Lt.M-19	43.255.196.36	Citrix Netscaler	nginx	11-Jul-2017
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.75	F5 BIG-IP	BigIP	28-Apr-2017
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.158	F5 BIG-IP	unknown	17-Apr-2017
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.138	FreeBSD	nginx	21-Oct-2014
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.138	FreeBSD	unknown	18-Aug-2014
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.138	FreeBSD	nginx	17-Aug-2014
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.138	FreeBSD	unknown	16-Aug-2014
PT. Telekomunikasi Selular Telkomsel Indonesia	202.3.208.138	FreeBSD	nginx	14-Aug-2014

Gambar 3

Sama seperti gambar 2, gambar 3 didapat dari hasil track pada tools netcraft.com, yang menampilkan hosting history yang berisi network owner, IP, OS dan web server yang digunakan serta waktu terakhir dilihat oleh owner.

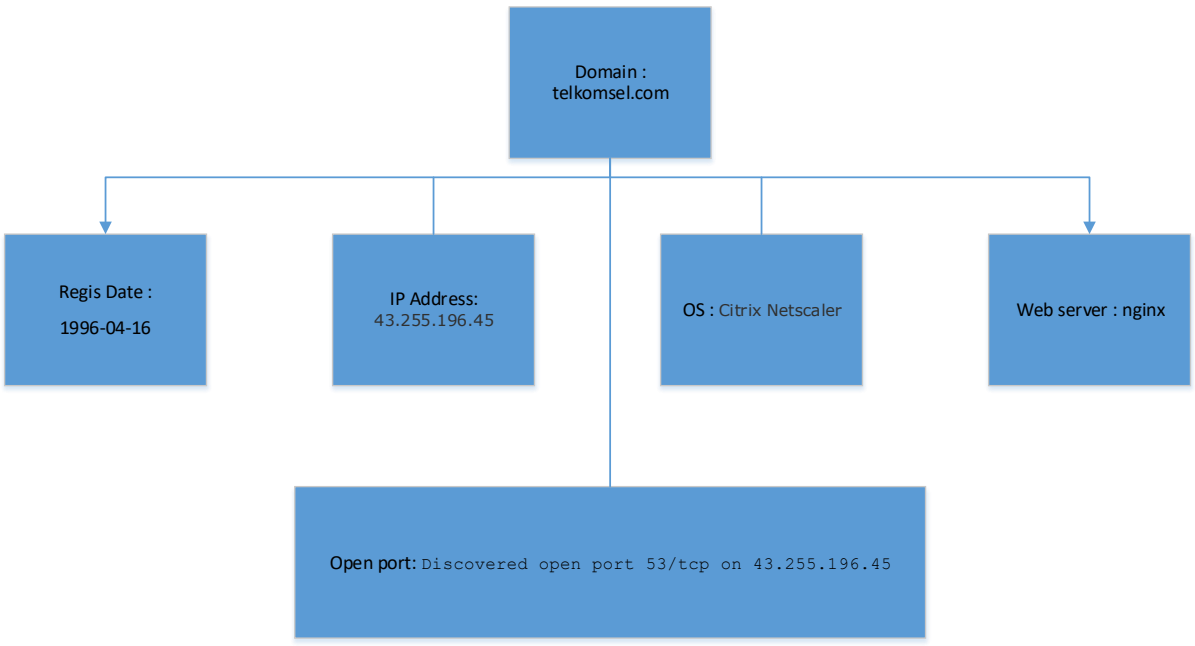
```
Scanning telkomsel.com (43.255.196.45) [1000 ports]
Discovered open port 53/tcp on 43.255.196.45
Completed SYN Stealth Scan at 09:01, 7.84s elapsed (1000 total ports)
```

Gambar 4

Gambar 4 didapat dari hasil track pada tools zenmap, dapat diketahui 1 port yang terbuka ialah

```
Discovered open port 53/tcp on 43.255.196.45
```

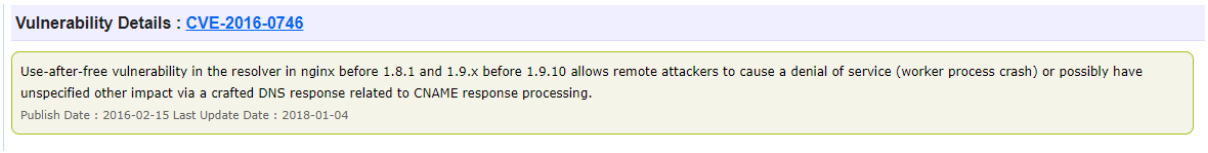
Kesimpulan data collection



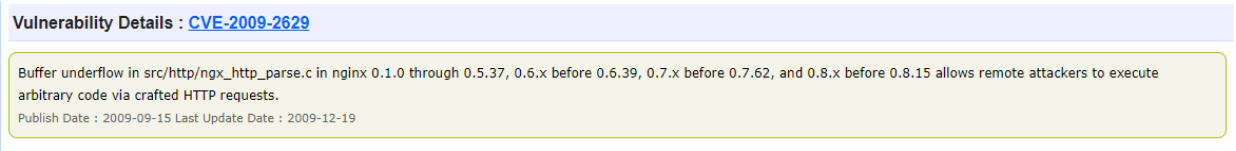
Vulnerabilities

Menggunakan cve details

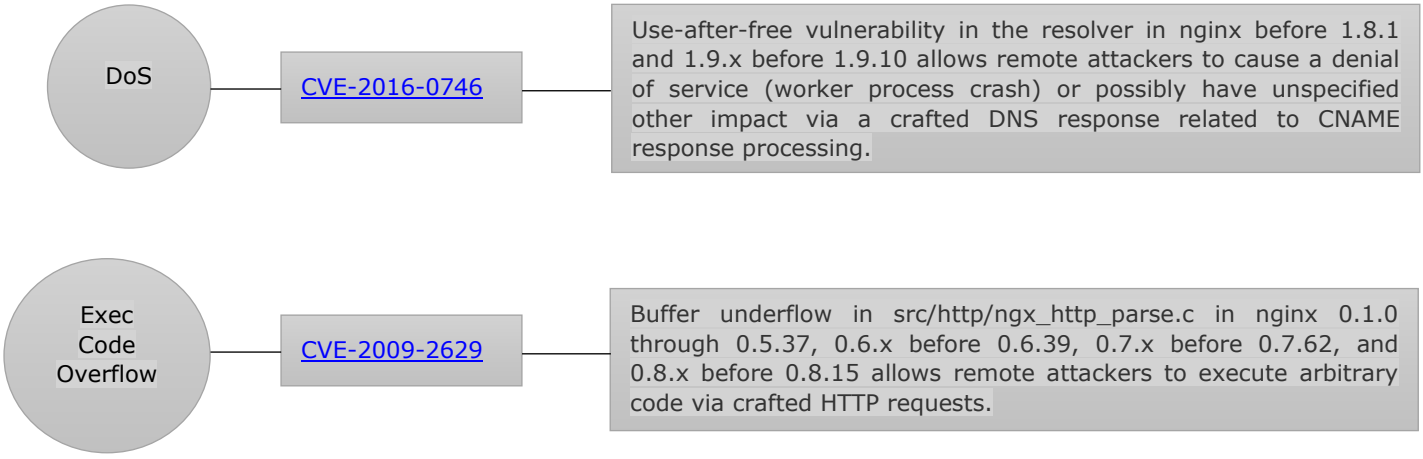
- Web server nginx :



Gunakan-setelah bebas kerentanan dalam resolver di nginx sebelum 1.8.1 dan 1.9.x sebelum 1.9.10 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (crash proses pekerja) atau mungkin memiliki dampak lain yang tidak ditentukan melalui respons DNS yang dibuat terkait dengan Pemrosesan respons CNAME



Buffer underflow di src / http / ngx_http_parse.c di nginx 0.1.0 sampai 0.5.37, 0.6.x sebelum 0.6.39, 0.7.x sebelum 0.7.62, dan 0.8.x sebelum 0.8.15 memungkinkan penyerang jarak jauh untuk mengeksekusi sewenang-wenang kode melalui permintaan HTTP dibuat.



Target : mpr.go.id

Data collection :

mpr.go.id

Updated 1 second ago

```
Domain ID:PANDI-DO284755
Domain Name:MPR.GO.ID
Created On:10-May-2000 13:35:17 UTC
Last Updated On:09-Jan-2017 07:22:10 UTC
Expiration Date:31-Jan-2019 23:59:59 UTC
Status:ok
Registrant ID:setjen-6633
Registrant Name:Setjen MPR
Registrant Organization:Sekretariat Jenderal MPR RI
Registrant Street1:Komplek MPR/DPR/DPD Jalan Gatot Subroto No.6
Registrant City:Jakarta Pusat
Registrant State/Province:DKI Jakarta
Registrant Postal Code:10270
Registrant Country:ID
Registrant Phone:+62.2157895063
Registrant FAX:+62.2157895261
Registrant Email:pdsi@setjen.mpr.go.id
```

Gambar 1

Domain informasi yang terlihat pada gambar 1 didapat dari hasil track pada tools whois.com

Background

Site title	Home | Majelis Permusyawaratan Rakyat	**Date first seen**	September 1998
Site rank		**Primary language**	Indonesian
Description	Website Resmi Majelis Permusyawaratan Rakyat Republik Indonesia (MPR RI)		
Keywords	mpr, republik indonesia, Fraksi, Foto, Pimpinan, Anggota, Info Lelang, Katalog Buku, Majalah, Agenda, Berita		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://mpr.go.id	**Netblock Owner**	PT Ikubaru Indonesia
Domain	mpr.go.id	**Nameserver**	ns10.dnsmadeeasy.com
IP address	103.219.249.44	**DNS admin**	dns@dnsmadeeasy.com
IPv6 address	*Not Present*	**Reverse DNS**	mpr.go.id
Domain registrar	*unknown*	**Nameserver organisation**	whois.wildwestdomains.com
Organisation	*unknown*	**Hosting company**	node.id
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	Enabled
Hosting country	ID		

Gambar 2

Sedangkan pada gambar 2, didapat dari hasil track pada tools netcraft.com yang menampilkan informasi background dan network.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT. Solusindo Bintang Pratama Internet Service Provider BATAM	103.29.7.87	Linux	Apache	6-Apr-2012
PT. Digital Wireless Indonesia ISP Gedung Cyber 7th Floor Jl. Kuningan Barat No 8, Jakarta 12710	118.82.1.89	Linux	Apache	25-Oct-2011
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.229	Linux	Apache/2.0.52 Red Hat	15-Jul-2011
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.12	Solaris 9/10	Apache/2.0.53 Unix PHP/4.3.11 mod_fastcgi/2.4.2	24-Apr-2008
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9/10	unknown	12-Apr-2005
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9/10	Apache/2.0.48 Unix PHP/4.3.4 mod_fastcgi/2.4.2	29-Mar-2005
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9/10	squid/2.5.STABLE6	28-Mar-2005
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9	squid/2.5.STABLE6	25-Jun-2004
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9	Apache/2.0.48 Unix PHP/4.3.4 mod_fastcgi/2.4.2	15-Jan-2004
PT Telekomunikasi Indonesia PT. Telkom Indonesia	202.134.0.12	Solaris 9	Apache/1.3.20 Unix mod_fastcgi/2.2.1 PHP/4.1.2	5-Oct-2003

Gambar 3

Sama seperti gambar 2, gambar 3 didapat dari hasil track pada tools netcraft.com, yang menampilkan hosting history yang berisi network owner, IP, OS dan web server yang digunakan serta waktu terakhir dilihat oleh owner.

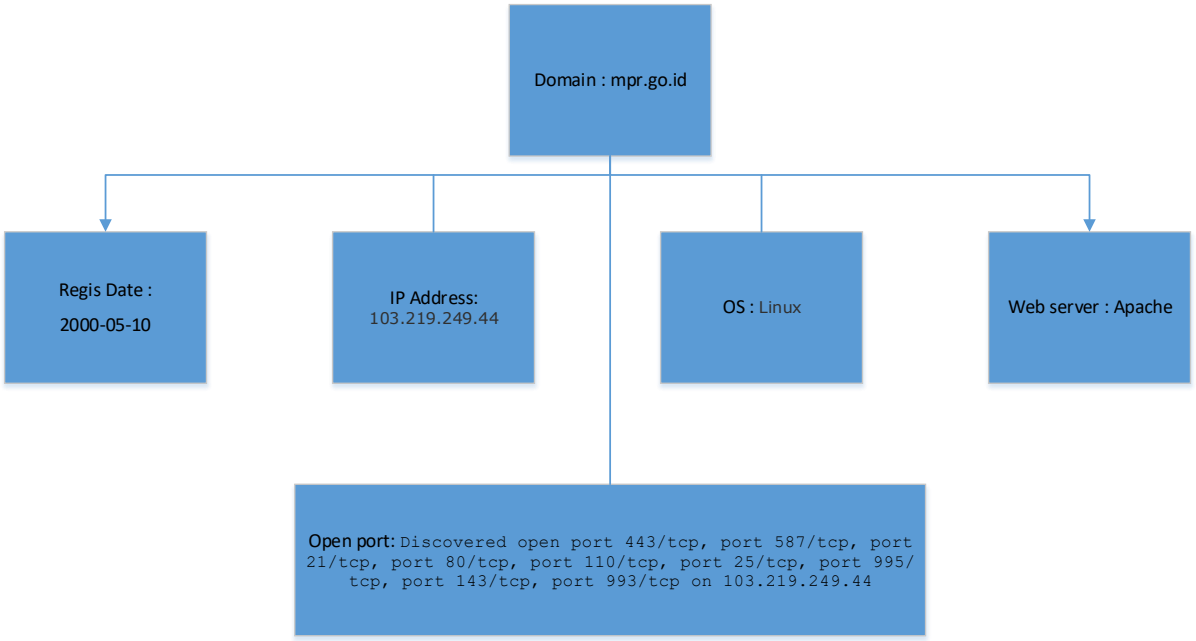
```
Scanning mpr.go.id (103.219.249.44) [1000 ports]
Discovered open port 443/tcp on 103.219.249.44
Discovered open port 587/tcp on 103.219.249.44
Discovered open port 21/tcp on 103.219.249.44
Discovered open port 80/tcp on 103.219.249.44
Discovered open port 110/tcp on 103.219.249.44
Discovered open port 25/tcp on 103.219.249.44
Discovered open port 995/tcp on 103.219.249.44
Discovered open port 143/tcp on 103.219.249.44
Discovered open port 993/tcp on 103.219.249.44
Increasing send delay for 103.219.249.44 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
```

Gambar 4

Gambar 4 didapat dari hasil track pada tools zenmap, dapat diketahui port yang terbuka ialah

```
Discovered open port 443/tcp on 103.219.249.44

Discovered open port 587/tcp on 103.219.249.44

Discovered open port 21/tcp on 103.219.249.44

Discovered open port 80/tcp on 103.219.249.44

Discovered open port 110/tcp on 103.219.249.44

Discovered open port 25/tcp on 103.219.249.44

Discovered open port 995/tcp on 103.219.249.44

Discovered open port 143/tcp on 103.219.249.44

Discovered open port 993/tcp on 103.219.249.44
```

Kesimpulan data collection



Vulnerabilities

Menggunakan cve details

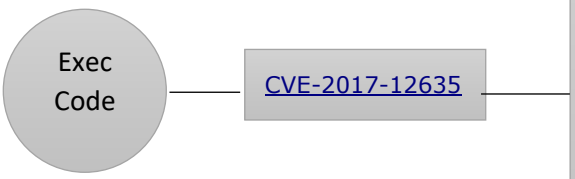
- Web server Apache :

Vulnerability Details : CVE-2017-12635

Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to submit _users documents with duplicate keys for 'roles' used for access control within the database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this can be used to give non-admin users access to arbitrary shell commands on the server as the database system user. The JSON parser differences result in behaviour that if two 'roles' keys are available in the JSON, the second one will be used for authorising the document write, but the first 'roles' key is used for subsequent authorization for the newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves admin privileges.

Publish Date : 2017-11-14 Last Update Date : 2018-02-03

Karena perbedaan parsel JSON berbasis Erlang dan parser JSON berbasis JavaScript, ada kemungkinan di Apache CouchDB sebelum 1.7.0 dan 2.x sebelum 2.1.1 untuk mengirimkan dokumen _users dengan kunci duplikat untuk 'peran' yang digunakan untuk kontrol akses dalam database, termasuk peran khusus '_admin', yang menunjukkan pengguna administratif. Dalam kombinasi dengan CVE-2017-12636 (Remote Code Execution), ini bisa digunakan untuk memberi akses pengguna non-admin ke perintah shell sewenang-wenang di server sebagai pengguna sistem database. Perbedaan parser JSON menghasilkan perilaku bahwa jika dua kunci 'peran' tersedia di JSON, kode kedua akan digunakan untuk memberi otorisasi pada penulisan dokumen, namun kunci 'peran' pertama digunakan untuk otorisasi berikutnya untuk pengguna yang baru dibuat. Dengan disain, pengguna tidak dapat menetapkan peran mereka sendiri. Kerentanan memungkinkan pengguna non-admin memberikan hak istimewa admin mereka sendiri.



CVE-2017-12635

Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to submit _users documents with duplicate keys for 'roles' used for access control within the database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this can be used to give non-admin users access to arbitrary shell commands on the server as the database system user. The JSON parser differences result in behaviour that if two 'roles' keys are available in the JSON, the second one will be used for authorising the document write, but the first 'roles' key is used for subsequent authorization for the newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves