KEAMANAN JARINGAN KOMPUTER

Reconnaissance Website

Oleh :

Nadya Rahma Noviyanti

09011281520127

Fakultas Ilmu Komputer

Jurusan Sistem Komputer

Universitas Sriwijaya

2019

1. WEBSITE PEMERINTAH

URL : http://www.indonesia.go.id

Web Server : Apache/2.4.6

BigIP

PHP/5.6.36

OS : Linux

Network

Site	http://www.indonesia.go.id	**Netblock Owner**	Kementerian Komunikasi dan Informasi Republik Indonesia
Domain	indonesia.go.id	**Nameserver**	ns1.setneg.go.id
IP address	202.89.117.193 (VirusTotal)	**DNS admin**	hostmaster@ns1.setneg.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Kementerian Komunikasi dan Informatika Republik Indonesia
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

CVE

Apache » Http Server » 2.4.6 : Security Vulnerabilities (Denial Of Service)

Cpe Name:*cpe:/a:apache:http_server:2.4.6*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15710	787		DoS	2018-03-26	2018-11-13	5.0	None	Remote	Low	Not required	None	None	Partial

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
2	CVE-2017-9788	20		DoS +Info	2017-07-13	2018-01-04	6.4	None	Remote	Low	Not required	Partial	None	Partial

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
3	CVE-2014-3523	399		DoS	2014-07-20	2018-01-04	5.0	None	Remote	Low	Not required	None	None	Partial

Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

Traceroute

#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Palembang	-2.9167	104.75	192.168.100.1		1	~	0	
2		Indonesia	Palembang	-2.9167	104.75	10.37.0.1		6	~	0	
3		*	*	-2.9167	104.75	*	*	0	<1	0	
4		*	*	-2.9167	104.75	172.16.2.249		15	~	0	
5		*	*	-2.9167	104.75	*	*	0	<1	0	
5		*	*	-2.9167	104.75	*	*	0	<1	0	
7		Indonesia	Jakarta	-6.1744	106.8294	218.100.36.25	telin.openixp.net	27	~	429	
8		Singapore	(Unknown)	1.3667	103.8	180.240.193....		14	~	904	
9		Indonesia	(Unknown)	-6.175	106.8286	202.89.117.1...		30	~	904	

2. WEBSITE DALAM NEGERI

URL : http://www.muhammadiyah.or.id

Web Server : Apache/2.4.6 CentOS PHP/5.4.16

Microsoft-IIS/5.0

Apache/1.3.34 Unix PHP/4.4.0

OS : Linux

Windows 2000

Windows Server 2003

FreeBSD

Network

Site	http://www.muhammadiyah.or.id	**Netblock Owner**	Universitas Muhammadiyah Malang
Domain	muhammadiyah.or.id	**Nameserver**	ns2.umm.ac.id
IP address	202.52.52.23 (VirusTotal)	**DNS admin**	root@ns2.umm.ac.id
IPv6 address	*Not Present*	**Reverse DNS**	muhammadiyah.or.id
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	umm.ac.id
Top Level Domain	Indonesia (.or.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

CVE

Apache » Http Server » 1.3.34 : Security Vulnerabilities (Denial Of Service)

Cpe Name:*cpe:/a:apache:http_server:1.3.34*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

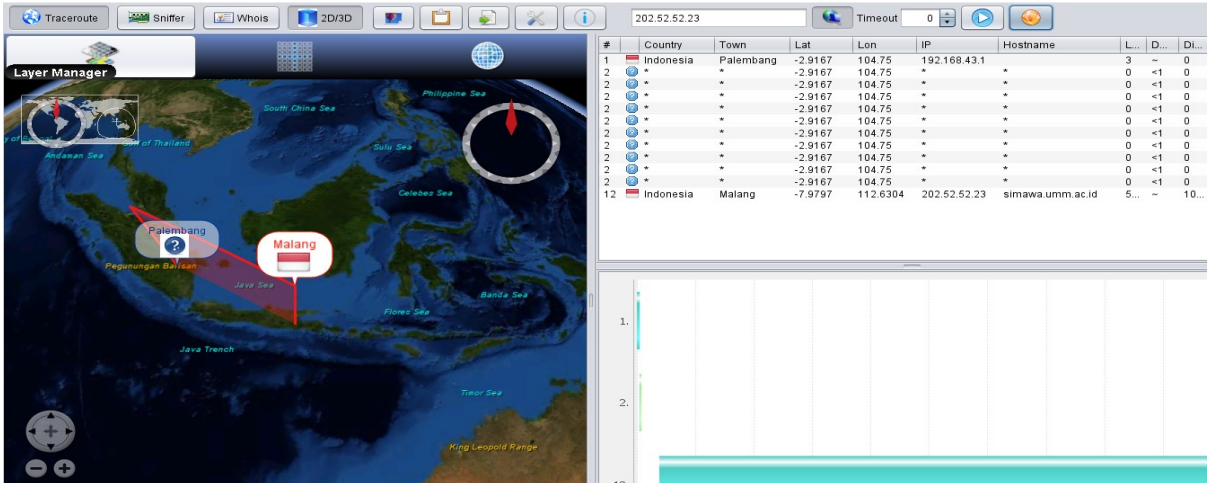
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2012-0031	399		DoS	2012-01-18	2018-01-17	4.6	None	Local	Low	Not required	Partial	Partial	Partial

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

2	CVE-2011-3348	399		DoS	2011-09-20	2017-12-28	4.3	None	Remote	Medium	Not required	None	None	Partial

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

Traceroute



3. WEBSITE LUAR NEGERI

URL : http://www.yahoo.com

Web Server : ATS

OS : Linux

Network

Site	http://www.yahoo.com	**Netblock Owner**	Yahoo! Europe
Domain	yahoo.com	**Nameserver**	ns1.yahoo.com
IP address	87.248.98.7 (VirusTotal)	**DNS admin**	hostmaster@yahoo-inc.com
IPv6 address	2a00:1288:110:1c:0:0:0:4	**Reverse DNS**	media-router-fp1.prod1.media.vip.ir2.yahoo.com
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	Oath Inc., 22000 AOL Way, Dulles, 20166, United States	**Hosting company**	Verizon
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	IE	**Latest Performance**	Performance Graph

CVE

Apache » Traffic Server » 6.2.0 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:traffic_server:6.2.0*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-8040	284			2018-08-29	2018-11-08	5.0	None	Remote	Low	Not required	None	Partial	None

Pages that are rendered using the ESI plugin can have access to the cookie header when the plugin is configured not to allow access. This affects Apache Traffic Server (ATS) versions 6.0.0 to 6.2.2 and 7.0.0 to 7.1.3. To resolve this issue users running 6.x should upgrade to 6.2.3 or later versions and 7.x users should upgrade to 7.1.4 or later versions.

2	CVE-2018-8022	20			2018-08-29	2018-10-17	5.0	None	Remote	Low	Not required	None	None	Partial

A carefully crafted invalid TLS handshake can cause Apache Traffic Server (ATS) to segfault. This affects version 6.2.2. To resolve this issue users running 6.2.2 should upgrade to 6.2.3 or later versions.

3	CVE-2018-8005	399			2018-08-29	2018-10-26	5.0	None	Remote	Low	Not required	None	None	Partial

When there are multiple ranges in a range request, Apache Traffic Server (ATS) will read the entire object from cache. This can cause performance problems with large objects in cache. This affects versions 6.0.0 to 6.2.2 and 7.0.0 to 7.1.3. To resolve this issue users running 6.x users should upgrade to 6.2.3 or later versions and 7.x users should upgrade to 7.1.4 or later versions.

Traceroute