Nama : Gonewaje
NIM : 09011181419005

TOP 5 CVE of Nginx

#	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-2009-2629	119		Exec Code Overflow	2009-09-15	2009-12-19	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Buffer underflow in src/http/ngx_http_parse.c in nginx 0.1.0 through 0.5.37, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.15 allows remote attackers to execute arbitrary code via crafted HTTP requests.														
2	CVE-2016-0746			DoS	2016-02-15	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Use-after-free vulnerability in the resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.														
3	CVE-2016-1247	59		+Priv	2016-11-29	2017-02-23	7.2	Admin	Local	Low	Not required	Complete	Complete	Complete
The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx ebuild before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.														
4	CVE-2009-3896	119		DoS Overflow	2009-11-24	2013-09-11	5.0	None	Remote	Low	Not required	None	None	Partial
src/http/ngx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.14 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a long URI.														
5	CVE-2010-2263	200		2 +Info	2010-06-15	2010-06-18	5.0	None	Remote	Low	Not required	Partial	None	None
nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or unparsed content of arbitrary files under the web document root by appending ::$DATA to the URI.														

1. CVE-2009-2629 (Buffer underflow/remote)

Pada urutan teratas untuk CVE dari Nginx adalah CVE yang cukup lama yaitu pada tahun 2009 dengan jenis vulnerability exceed buffer underflow dan mendapatkan skor 7.5. Buffer underflow berbeda dengan buffer overflow dimana buffer overflow bekerja dengan cara "membanjiri" program dengan input an, buffer underflow bekerja dimana ketika input yang dimasukkan lebih sedikit/lambat daripada input yang seharusnya sehingga membuat ruang buffer kosong dan menyebabkan program terputus-putus. Namun kelemahan ini sudah lama pula diatasi karena vuln pada CVE ini hanya bekerja pada nginx versi dibawah 0.8.14 dan sekarang nginx terbaru adalah versi 1.13.9 dan pada saat itu solusi yang ditawarkan adalah dengan melakukan patching program. Vulnerability pada CVE ini memungkinkan penyerang untuk melakukan remote akses melalui HTTP request.

2. CVE-2016-0746 (DoS/remote)

CVE ini dapat dikatakan masih terbilang baru karena menginfeksi nginx versi 1.8.0 – 1.9.9, vulnerability dari CVE ini digolongkan sebagai serangan DoS (Denial of Service) adalah sebuah serangan yang bekerja dengan cara menghabiskan resource yang dimiliki oleh komputer sehingga komputer tersebut tidak dapat menjalankan tugasnya dengan benar. CVE ini 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.

Nama : Gonewaje
NIM : 09011181419005

3. **CVE-2016-1247 (smylink/local)**

   CVE ini memungkinkan pengguna lokal mengakses akun pengguna server web untuk mendapatkan hak istimewa root melalui serangan symlink pada log kesalahan. serangan ini bergantung pada direktori /var/log/nginx yang dimiliki oleh www-data, dan logrotate disempurnakan dengan benar pada mesin. Jenis serangan ataupun teknik yang digunakan pada CVE ini adalah symlink yaitu attacker mengincar file-file konfigurasi yang tidak terproteksi dengan baik yang pada kasus CVE ini mengincar file konfigurasi pada direktori /var/log/nginx yang dimiliki oleh www-data. Hal yang membuat CVE ini menempati urutan ke-3 dengan skor 7.2 adalah dengan teknik symlink, attacker bisa mendapatkan hak akses penuh/admin sehingga dapat melakukan sesuatu hal sesuka mereka pada server tersebut.

4. **CVE-2009-3896 (DoS overflow/remote)**

   CVE yang sudah cukup lama dan menempati urutan ke-4 ini mendapat skor 5.0 dengan jenis vulnerability DoS overflow yang menyebabkan null pointer dereference. Null pointer dereference meningkatkan NullPointerException, biasanya merupakan hasil dari satu atau lebih asumsi programmer yang dilanggar. Sebagian besar masalah null pointer mengakibatkan masalah keandalan perangkat lunak secara umum, namun jika penyerang dengan sengaja dapat memicu dereference pointer null, penyerang mungkin dapat menggunakan pengecualian yang dihasilkan untuk mengabaikan logika keamanan atau menyebabkan aplikasi tersebut mengungkapkan informasi debug yang akan berharga. dalam merencanakan serangan selanjutnya.
   Dereference null-pointer terjadi ketika sebuah pointer dengan nilai NULL digunakan seolah-olah menunjuk ke area memori yang valid. Solusi yang ditawarkan untuk mencegah CVE ini adalah dengan melakukan update patch, dengan adanya CVE ini pada masanya setidaknya telah berdampak pada 283 aplikasi nginx.

5. **CVE-2010-2263 (injection/remote)**

   dimana Nginx versi 0.8 sebelum 0.8.40 dan 0.7 sebelum 0.7.66, saat berjalan di OS Windows yang memungkinkan penyerang jarak jauh mendapatkan kode sumber atau konten yang tidak dipasteile dari file sewenang-wenang dari induk web dengan menambahkan ::$DATA ke URL. Dampak dari adanya celah oleh CVE-2010-2263 menyebabkan setidaknya 160 aplikasi berdampak kepada produk mereka sendiri yaitu Nginx beruntun kepada versi-versi sebelumnya.

Nama : Gonewaje
NIM : 09011181419005