Tugas Keamanan Jaringan Komputer

War-Driving Operating System CVE Linux

Disusun Oleh:

Tamara Kharisma Restu (09011281419045)

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

-Vulnerability Details : CVE-2017-1000410

Linux kernel version 3.3-rc1 dan seterusnya

Dipengaruhi oleh kerentanan terletak pada pemrosesan perintah L2CAP yang masuk - ConfigRequest, dan ConfigResponse messages. Informasi kebocoran ini adalah hasil dari variabel tumpukan yang tidak diinisiasi yang dapat dikembalikan ke penyerang dalam keadaan tidak diinisiasi mereka. Dengan memanipulasi arus kode yang mendahului penanganan pesan konfigurasi ini, penyerang juga dapat memperoleh kontrol atas data mana yang akan disimpan di variabel tumpukan yang tidak diinisiasi. Hal ini memungkinkan dia untuk melewati KASLR, dan stack canaries protection karena kedua pointer dan stack canaries mungkin bocor dengan cara ini.

Menggabungkan kerentanan ini (misalnya) dengan kerentanan RCE yang sebelumnya diungkapkan dalam penguraian konfigurasi L2CAP (CVE-2017-1000251) memungkinkan penyerang mengeksploitasi RCE terhadap kernel yang dibangun dengan mitigasi di atas. Ini adalah spesifik dari kerentanan ini: Dalam fungsi l2cap_parse_conf_rsp dan dalam fungsi l2cap_parse_conf_req variabel berikut dideklarasikan tanpa inisialisasi: struct l2cap_conf_efs efs; Sebagai tambahan, ketika mengurai parameter konfigurasi masukan di kedua fungsi ini, kasus saklar untuk menangani elemen EFS dapat melewatkan panggilan memcpy yang akan menulis ke variabel efs: ... kasus L2CAP_CONF_EFS: if (olen == sizeof (efs)) memcpy (& efs, (void *) val, olen); ... olen di atas jika penyerang dikendalikan, dan terlepas dari itu jika, dalam kedua fungsi ini, variabel efs akhirnya akan ditambahkan ke permintaan konfigurasi keluar yang sedang dibangun: l2cap_add_conf_opt (& ptr, L2CAP_CONF_EFS, sizeof (efs), (unsigned long) & efs);

Jadi dengan mengirimkan permintaan konfigurasi, atau respons, yang mengandung elemen L2CAP_CONF_EFS, namun dengan panjang elemen yang tidak sizeof (efs) - variabel yang memcpy terhadap variabel efs yang tidak diinisiasi dapat dihindari, dan variabel yang tidak diinisiasi akan dikembalikan ke penyerang. (16 byte).

- 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)	Bypass a restriction or similarObtain Information
CWE ID	200

- Products Affected By CVE-2017-1000410

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Linux	Linux Kernel	3.3	RC5			Version Details Vulnerabilities
2	OS	Linux	Linux Kernel	3.3				Version Details Vulnerabilities
3	OS	Linux	Linux Kernel	3.3	RC6			Version Details Vulnerabilities
4	OS	Linux	Linux Kernel	3.3	RC1			Version Details Vulnerabilities
5	OS	Linux	Linux Kernel	3.3	RC7			Version Details Vulnerabilities
6	OS	Linux	Linux Kernel	3.3	RC2			Version Details Vulnerabilities
7	OS	Linux	Linux	3.3	RC3			Version

			Kernel			Details Vulnerabilities
8	OS	Linux	Linux Kernel	3.3	RC4	Version Details Vulnerabilities
9	OS	Linux	Linux Kernel	3.3.1		Version Details Vulnerabilities
10	OS	Linux	Linux Kernel	3.3.2		Version Details Vulnerabilities
11	OS	Linux	Linux Kernel	3.3.3		Version Details Vulnerabilities
12	OS	Linux	Linux Kernel	3.3.4		Version Details Vulnerabilities
13	OS	Linux	Linux Kernel	3.3.5		Version Details Vulnerabilities
14	OS	Linux	Linux Kernel	3.3.6		Version Details Vulnerabilities
15	OS	Linux	Linux Kernel	3.3.7		Version Details Vulnerabilities
16	OS	Linux	Linux Kernel	3.3.8		Version Details Vulnerabilities

Maximum 700 results are displayed even if there are more. A very little number of cve entries, mostly related to cisco products and google chrome , affect even more than 700 different versions but they are not displayed to keep page size within reasonable limits. Affected product count numbers may not reflect the actuals numbers either.

- Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Linux	Linux Kernel	700