KEAMANAN JARINGAN KOMPUTER

“COMMON VULNERABILITIES AND EXPOSURES”

Analisis Serangan dari 5 Hole pada CVE

Disusun oleh :

Henny Pratiwi (09011281520129)

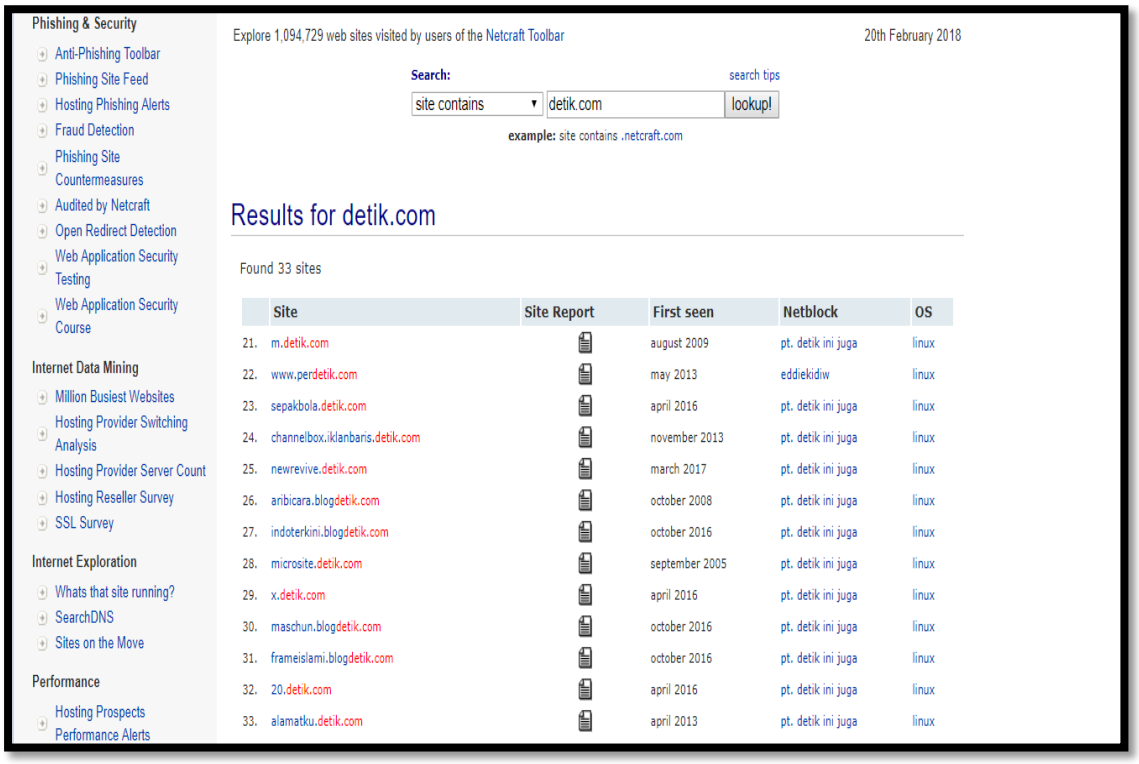
SISTEM KOMPUTER

FASILKOM INDERALAYA

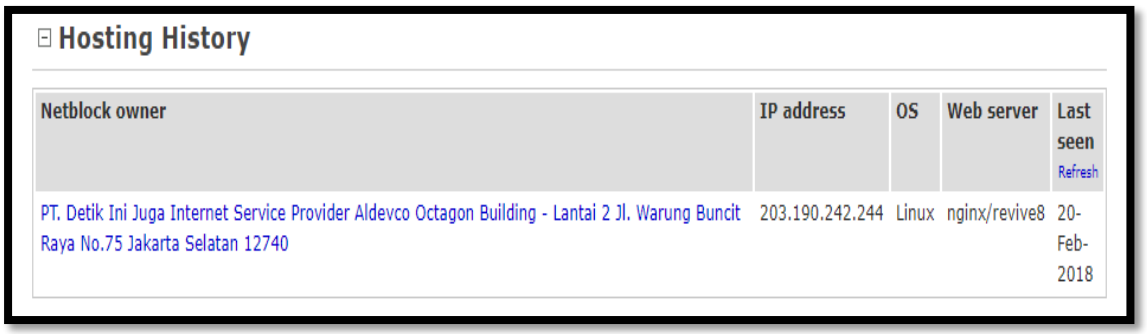
UNIVERSITAS SRIWIJAYA

2018

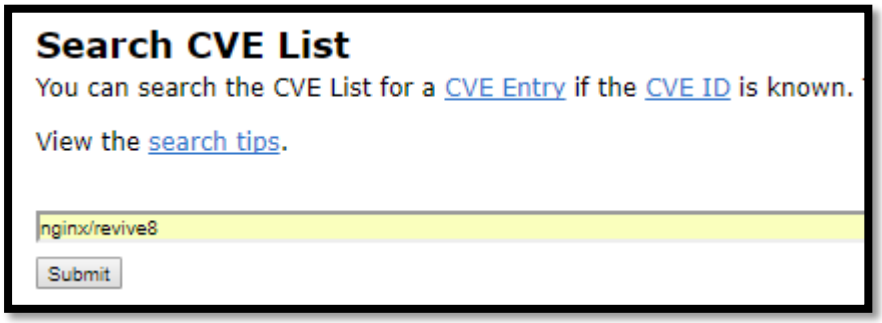
1. Deskripsi hasil pencarian hole pada system DNS (detik.com)
   Menggunakan netcraft.com



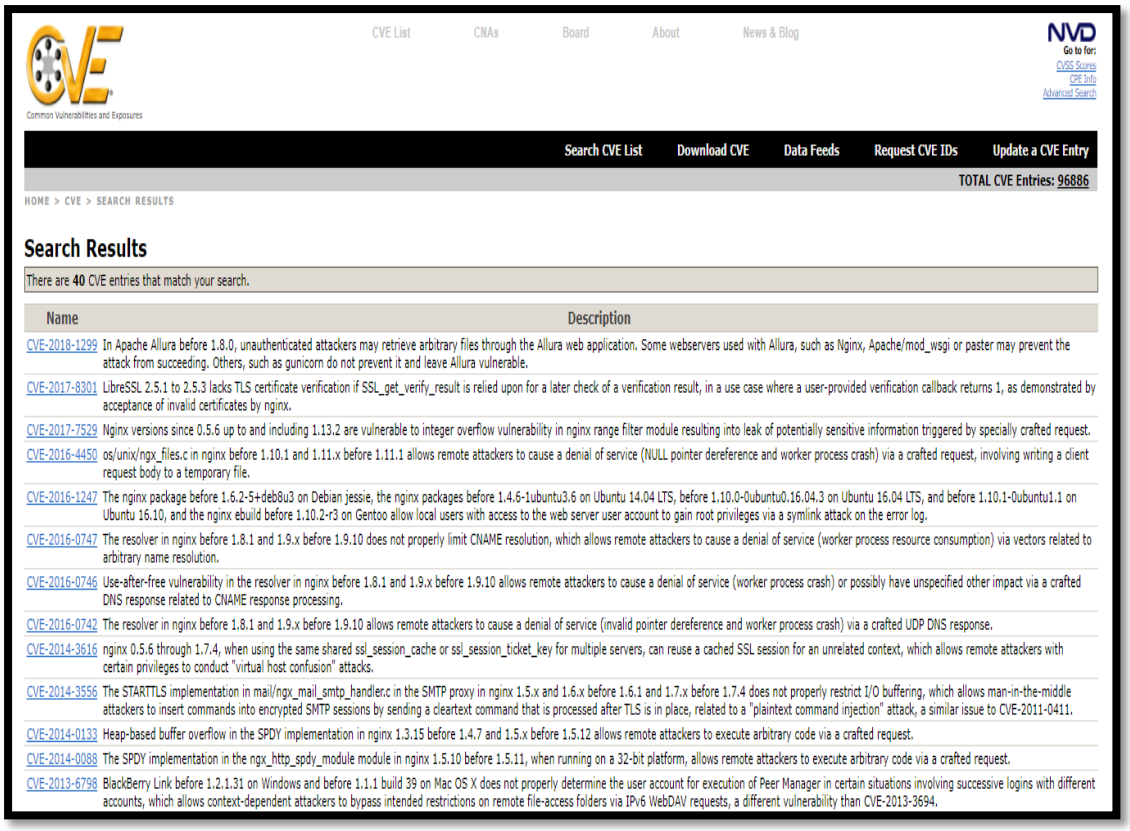
Klik site report pada maret 2017 site number 25 dan lihat hosting historynya lalu aka nada penjelasan pada web servernya ”nginx/revive8”



Lalu buka cve.mitre.org pada bagian search cve list masukan ”nginx/revive8”



Maka aka nada tampilan berikut setelah mengklik submit



CVE List CNAs Board About News & Blog

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Common Vulnerabilities and Exposures

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 96886

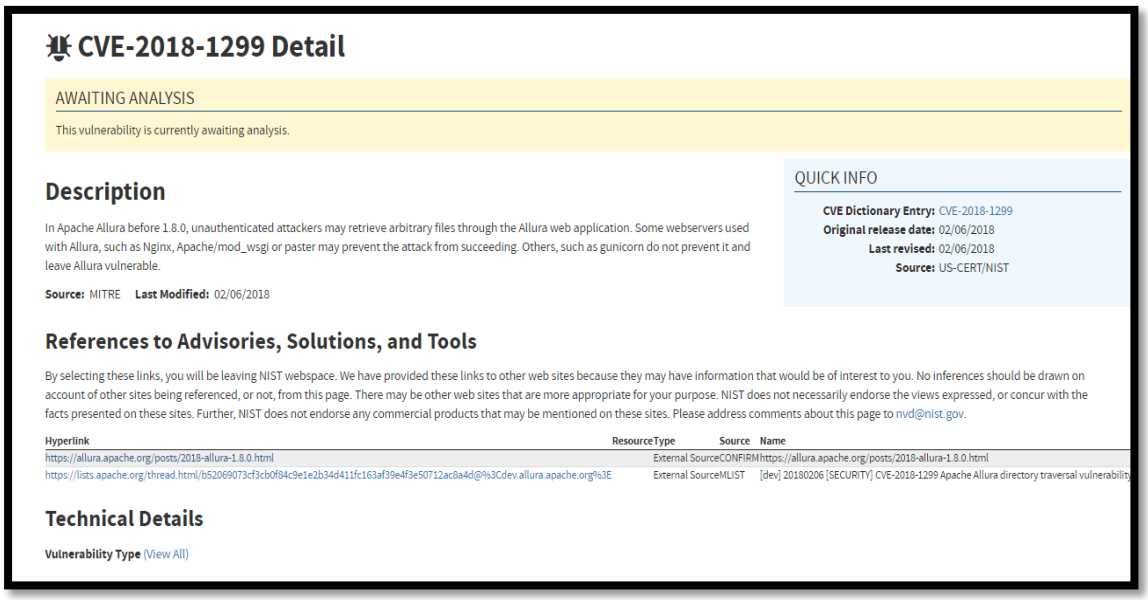
HOME > CVE > SEARCH RESULTS

Search Results

There are **40** CVE entries that match your search.

Name	Description
CVE-2018-1299	In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some webservers used with Allura, such as Nginx, Apache/mod_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable.
CVE-2017-8301	LibreSSL 2.5.1 to 2.5.3 lacks TLS certificate verification if SSL_get_verify_result is relied upon for a later check of a verification result, in a use case where a user-provided verification callback returns 1, as demonstrated by acceptance of invalid certificates by nginx.
CVE-2017-7529	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
CVE-2016-4450	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.
CVE-2016-1247	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.
CVE-2016-0747	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.
CVE-2016-0746	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.
CVE-2016-0742	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 (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.
CVE-2014-3616	nginx 0.5.6 through 1.7.4, when using the same shared ssl_session_cache or ssl_session_ticket_key for multiple servers, can reuse a cached SSL session for an unrelated context, which allows remote attackers with certain privileges to conduct "virtual host confusion" attacks.
CVE-2014-3556	The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.
CVE-2014-0133	Heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request.
CVE-2014-0088	The SPDY implementation in the ngx_http_spdy_module module in nginx 1.5.10 before 1.5.11, when running on a 32-bit platform, allows remote attackers to execute arbitrary code via a crafted request.
CVE-2013-6798	BlackBerry Link before 1.2.1.31 on Windows and before 1.1.1 build 39 on Mac OS X does not properly determine the user account for execution of Peer Manager in certain situations involving successive logins with different accounts, which allows context-dependent attackers to bypass intended restrictions on remote file-access folders via IPv6 WebDAV requests, a different vulnerability than CVE-2013-3694.

2. Analisis Hole
HOLE 1



CVE-2018-1299 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some webservers used with Allura, such as Nginx, Apache/mod_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable.

Source: MITRE **Last Modified:** 02/06/2018

QUICK INFO

CVE Dictionary Entry: CVE-2018-1299
Original release date: 02/06/2018
Last revised: 02/06/2018
Source: US-CERT/NIST

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

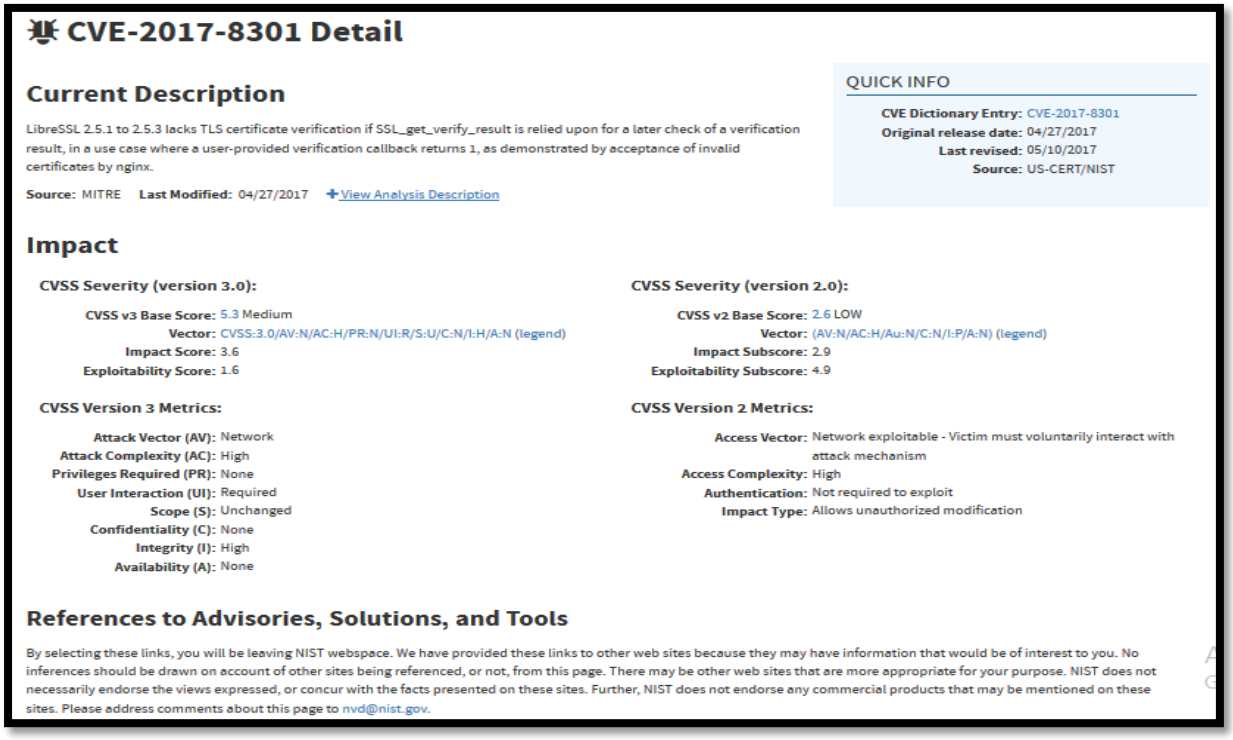
Hyperlink	ResourceType	Source	Name
https://allura.apache.org/posts/2018-allura-1.8.0.html	External Source	CONFIRM	https://allura.apache.org/posts/2018-allura-1.8.0.html
https://lists.apache.org/thread.html/b52069073cf3cb0f84c9e1e2b34d411fc163af39e4f3e50712ac8a4d@%3Cdev.allura.apache.org%3E	External Source	MLIST	[dev] 20180206 [SECURITY] CVE-2018-1299 Apache Allura directory traversal vulnerabilit

Technical Details

Vulnerability Type (View All)

Pada kali ini mendiskripsikan hole mengenai : Di Apache Allura sebelum 1.8.0, penyerang yang tidak diautentikasi dapat mengambil file yang sewenang-wenang melalui aplikasi web Allura. Beberapa webserver yang digunakan dengan Allura, seperti Nginx, Apache / mod_wsgi atau paster dapat mencegah serangan dengan berhasil. Yang lainnya, seperti gunicorn tidak mencegahnya dan membiarkan Allura rentan.

HOLE 2 :



CVE-2017-8301 Detail

Current Description

LibreSSL 2.5.1 to 2.5.3 lacks TLS certificate verification if SSL_get_verify_result is relied upon for a later check of a verification result, in a use case where a user-provided verification callback returns 1, as demonstrated by acceptance of invalid certificates by nginx.

Source: MITRE **Last Modified:** 04/27/2017 +View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2017-8301
Original release date: 04/27/2017
Last revised: 05/10/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 5.3 Medium
Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N (legend)
Impact Score: 3.6
Exploitability Score: 1.6

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): Required
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): High
Availability (A): None

CVSS Severity (version 2.0):

CVSS v2 Base Score: 2.6 LOW
Vector: (AV:N/AC:H/Au:N/C:N/I:P/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 4.9

CVSS Version 2 Metrics:

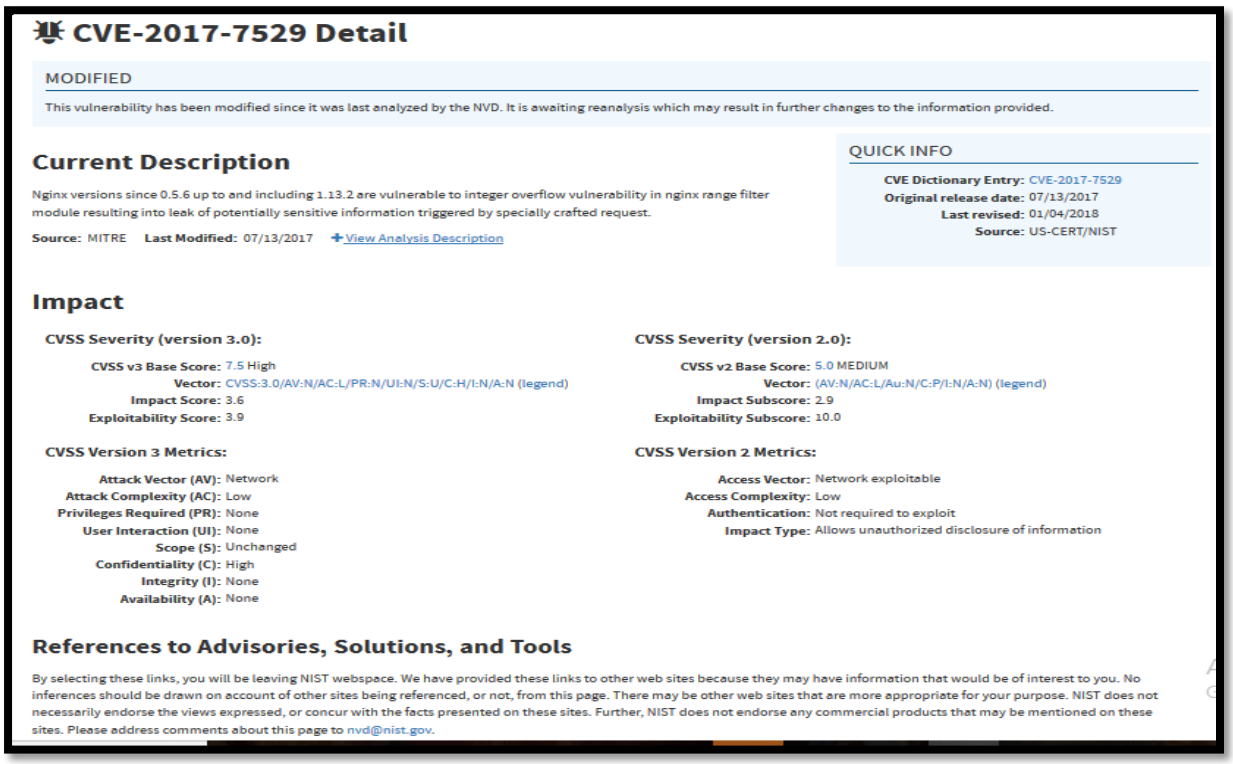
Access Vector: Network exploitable - Victim must voluntarily interact with attack mechanism
Access Complexity: High
Authentication: Not required to exploit
Impact Type: Allows unauthorized modification

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Tidak memiliki verifikasi sertifikat TLS jika SSL_get_verify_result diandalkan untuk pemeriksaan hasil verifikasi nanti, dalam kasus penggunaan di mana pengembalian verifikasi yang diberikan pengguna kembali semula, seperti yang ditunjukkan oleh penerimaan sertifikat tidak sah oleh nginx.

HOLE 3 :



CVE-2017-7529 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

Source: MITRE **Last Modified:** 07/13/2017 +View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2017-7529
Original release date: 07/13/2017
Last revised: 01/04/2018
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.5 High
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (legend)
Impact Score: 3.6
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): None
Availability (A): None

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

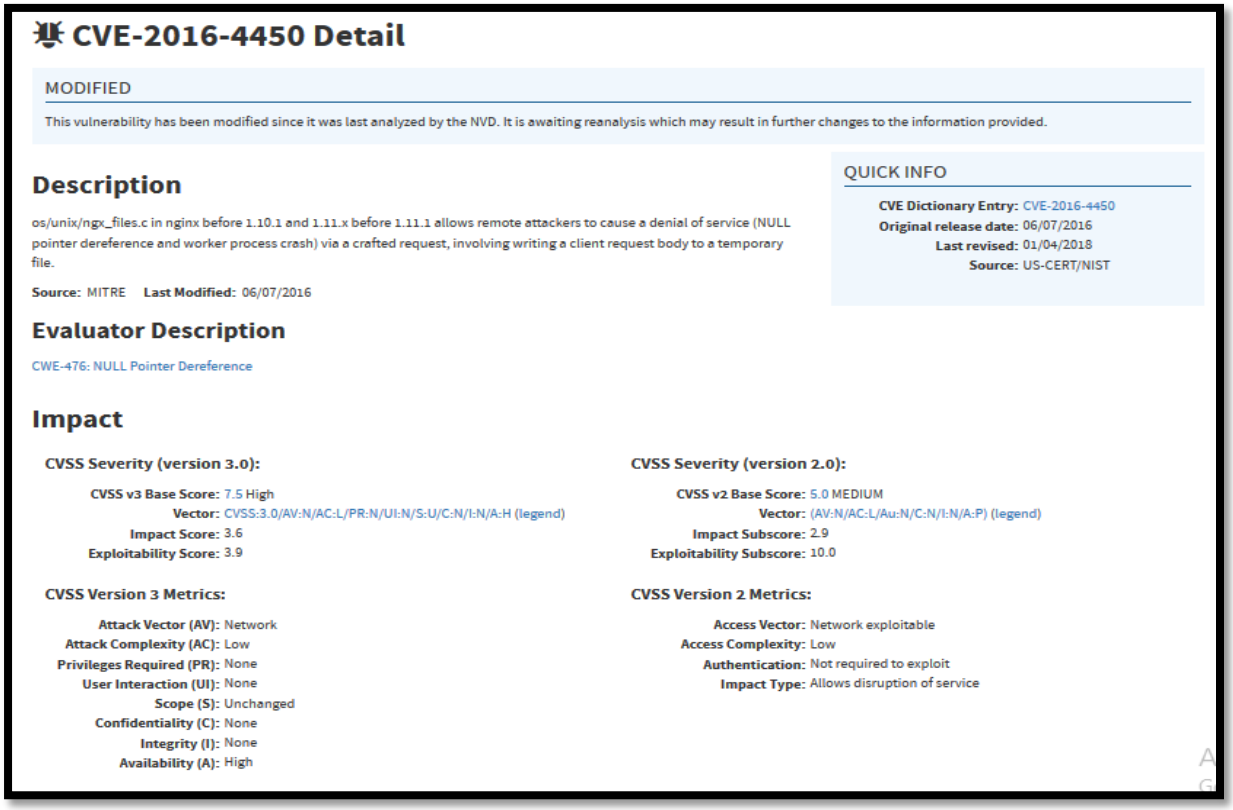
Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Versi Nginx sejak 0.5.6 sampai dan termasuk 1.13.2 rentan terhadap kerentanan overflow integer dalam modul filter rentang nginx yang mengakibatkan bocornya informasi sensitif yang dipicu oleh permintaan yang dibuat secara khusus.

HOLE 4 :



CVE-2016-4450 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.

Source: MITRE **Last Modified:** 06/07/2016

QUICK INFO

CVE Dictionary Entry: CVE-2016-4450
Original release date: 06/07/2016
Last revised: 01/04/2018
Source: US-CERT/NIST

Evaluator Description

CWE-476: NULL Pointer Dereference

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.5 High
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (legend)
Impact Score: 3.6
Exploitability Score: 3.9

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P) (legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

CVSS Version 3 Metrics:

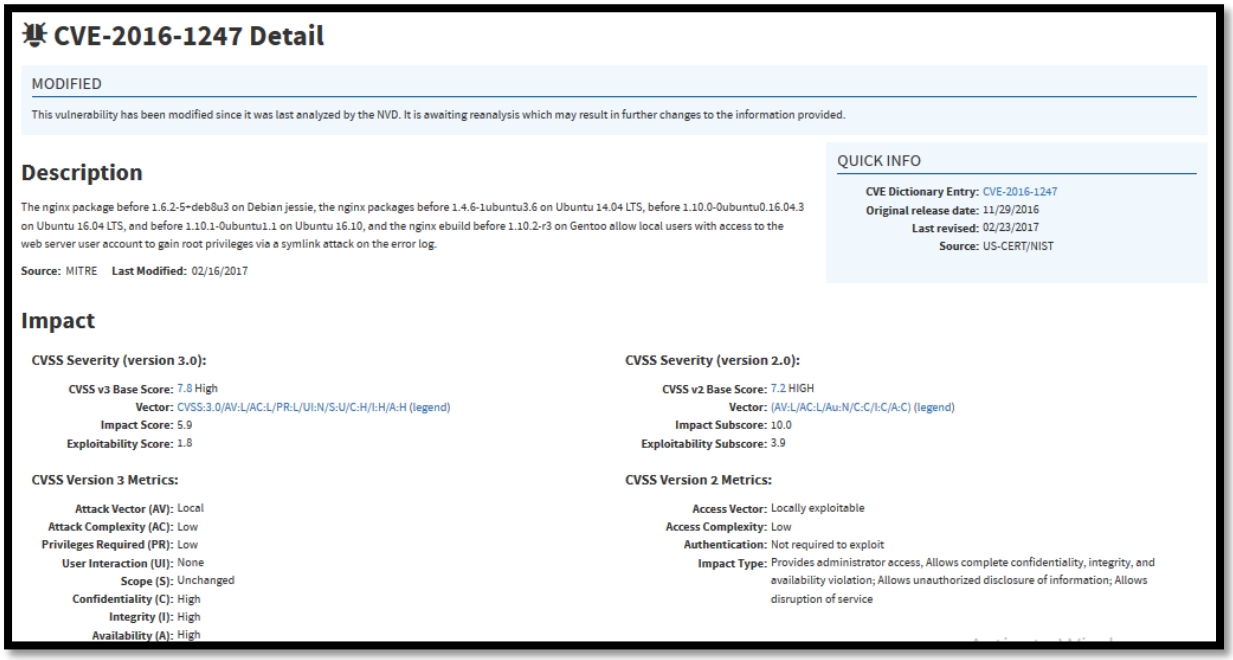
Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): None
Availability (A): High

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows disruption of service

Os/unix/ ngx_files.c di nginx sebelum 1.10.1 dan 1.11.x sebelum 1.11.1 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (NULL pointer dereference dan crash proses pekerja) melalui permintaan yang dibuat, yang melibatkan penulisan permintaan klien ke file sementara.

HOLE 5:



CVE-2016-1247 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

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.

Source: MITRE **Last Modified:** 02/16/2017

QUICK INFO

CVE Dictionary Entry: CVE-2016-1247
Original release date: 11/29/2016
Last revised: 02/23/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 7.8 High
Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 1.8

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.2 HIGH
Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 3.9

CVSS Version 3 Metrics:

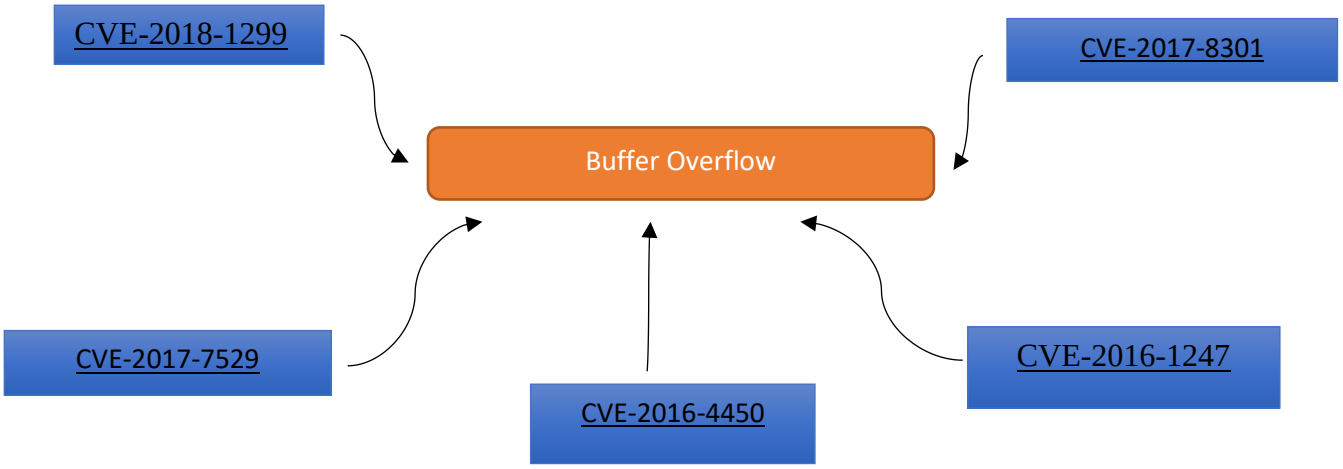
Attack Vector (AV): Local
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Version 2 Metrics:

Access Vector: Locally exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

memungkinkan pengguna lokal mengakses akun pengguna server web untuk mendapatkan hak istimewa root melalui serangan symlink pada log kesalahan.

Scema permasalahan pada 5 hole adalah :

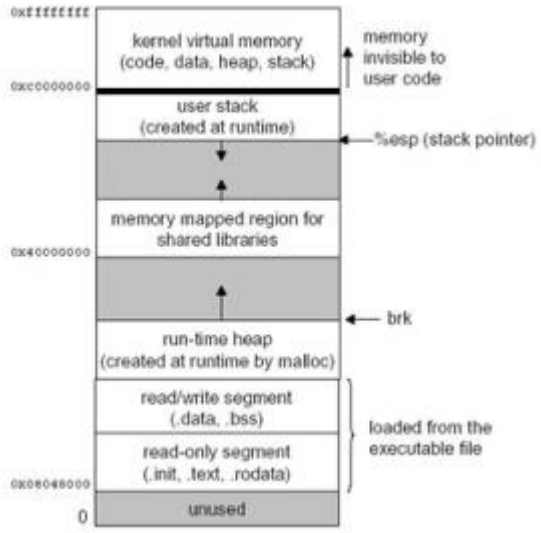


Kelemahan Buffer overflow adalah salah satu dari banyak kelemahan dari keamanan komputer.Kelemahan jenis ini dapat digunakan pada remote access atau local access, karena ini dapat memberikan si Attacker kesempatan untuk melanjarkan jurus-jurus dengan koding dikomputer target.
Serangan Buffer overflow terjadi ketika si Attacker memberikan input yang berlebihan pada program yang di jalankan, sehingga program mengalami kelebihan muatan dan memory tidak dapat mengalokasikannya. Ini memberikan kesempatan kepada Attacker untuk menindih data pada program dan men-takeover kontroll program yang dieksekusi attacker.
Buffee overflow hasil dari dari kelemahan bahasa pemrograman c, c++, fortran, dan assembly, yang tidak secara otomatis melakukan pengecekan batas input ketika program dieksekusi. Sebagai akibat dari Buffer overflow dapat menyebatkan crash pada program, atau mempersilahkan si Attacker untuk mengeksekusi perintah atau koding jahatnya untuk menguasai sistem target, seperti tujuan mengambil alih akun root menggunakan metode Buffer overflow.
ibaratnya seperti ini,,
si Attacker : Kamu akan saya hipnotis, tidur lebih dalam dan lebih lelap dari pada sebelumnya,,,
si Program : monggo mas Attacker silahkan, diapakan saja, aku rela,,,,
Di dalam artikel ini, saya mencoba sedikit memberikan penjelasan bagaimana buffer overflow itu bekerja, dan bagaimana cara mengatisipasinya. Buffer overflow biasa terjadi karena sebagai berikut ;

- Program yang begitu kompleks, sehinnga programmer sendiri tidak mengetahui kelemahan programnya
- Relies on external data to control pada program

Buffer adalah alokasi yang disediakan di memory seperti array atau pointer di C. di bahasa C dan C++, tidak ada pembatasan otomatis pada buffernya, yang mana user dapat menulis input melewati buffer.
Program bahasa C diatas adalah program yang valid, dan setiap compiler dapat mengkompil ini tanpa error. Tetapi, program ini dapat dijahili dengan menuliskan input melebihi batas buffer memory yang telah ditentukan, yang mana akan menghasilkan kesalahan pada program.

Sebuah proses adalah program dalam eksekusi. Program yang tereksekusi di dalam disk mengandung beberapa set instruksi binary yang di kerjakan oleh prosessor; beberapa read-only data, seperti printf string format; global dan data statis yang output terakhir eksekusi program; and sebuah brk pointer yang menjaga jalur dari malloced memory. Fungsi local variabel adalah otomatisasi terbentuknya variabel dalam stack ketika fungsi di eksekusi.

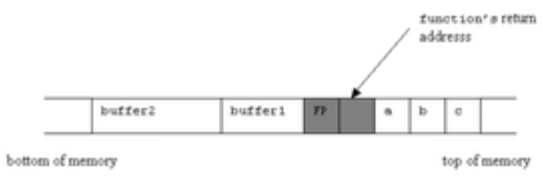


Ilustrasi di atas memperlihatkan layout memory di Linux. Sebuah proses dimulai dengan koding program-program dan data. Kode dan data berada dalam instruksi prgram dan inisialisasi dan uninialisasi statis dan global data secara berturut-turut. Setelah itu adalah run-time heap (Dibuat menggunakan malloc/calloc), dan di posisi atas adalah users stack. Stack ini digunakan ketika sebuah fungsi di panggil.

Bagian Stack.
Stack adalah beberapa blok dari memory yang berisi data. Sebuah stack pointer (SP) menunjuk paling atas dalam stack. Ketika pemanggilan fungsi terbentuk, parameter fungsi masuk ke dalam stack dari kanan ke kiri. Kemudian alamat pengembalian nilai (alamat yang akan dieksekusi setelah pengembalian nilai fungsi yang ditunjuk oleh frame pointer (FP), masuk ke dalam stack. Frame pointer digunakan sebagai referensi variabel lokal dan parameter fungsi, karena itu semua adalah kesatuan dari FP.

Ilustrasi di atas adalah bagian-bagian dari stack ketika sebuah fungsi dieksekusi. Perhatikan FP berada di antar local dan return addresses.

function stack seperti di bawah ini;



Seperti yang anda lihat, buffer1 menggunakan 8 bytes dan buffer2 12 byter, di memory dapat dialamatkan hanya dalam beberapa bytes (4 byters). Sebagai tambahan, FP digunakan untuk mengakses variabel a,b,c, buffer1 dan buffer2. Semua variabel di bersihkan dalam stack sebagai function terminates. Variabel tersebut tidak mengambil space dalam disk copy eksekusi.

Program ini dijamin setelah di kompil, akan menghasilkan error, karena string (str) sebesar 27 bytes terkopi ke dalam lokasi (buffer) yang hanya dialokasikan sebesar 16 bytes. Ekstra bytes melewati buffer dan menimpa ruang yang dialokasikan untuk FP, return address juga terkena. Hal ini, menyebabkan corrupt dalam proses stack. Funsi yang digunakan untuk kopi string adalah strcpy, yang tidak memeriksa batasan inputnya. Menggunakan strncpy akan menghindari kejadian ini di dalam stack. Bagaimanapun, contoh klasik ini, menunjukkan bagaimana konsep buffer overflow dalam menimpa sebua fungsi return address, dan dilanjutkan dengan menjalankan beberapa malicious code.

Overwriting Function's Return Addresses

Seperti yang kita tahu, sangat mudah untuk melakukan overwriting function's return addresses, Attacker menggunakan teknik buffer overflow untuk mendapatkan akses root. Attacker mencoba mengeksekusi buffer overflowwing area, menimpa nilai dari return address yang mengisi nilai ke buffer dan mengeksekusi kode jahatnya. Seperti kode yang bisa dimasukkan ke dalam program menggunakan environment variables atau program input parameters. Sebagai contoh koding yang bisa mendapatkan shell akun root pada paper yang ditulis oleh Aleph One untu Phrack Magazine di http://destroy.net/machines/security/P49-14-Aleph-One males juga untuk diceritakan lagi.

Tindakan Untuk Mencegah Buffer Overflow.

Tidak ada satupun metode yang dijelaskan di bawah yang benar-benar bisa mencegah kemungkinan serangan, namanya juga manusia tempatnya salah dan lupa. Tetapi metode di bawah ini, dapat meminimalisir dari kegiatan buffer overflows yang mengakibatkan kerusakan stack.

1. Menulis kode yang aman : Buffer overflow adalah hasil dari input yang berlebihan ke dalam buffer. C library seperti strcpy(), strcat(), sprintf() dan vsprintf() beroperasi pada null terminated strings dan tidak mengecek batasan input. gets() juga fungsi lainnya yang memasukkan input ke dalam buffer dari stdin. Pada scanf() juga bisa mengakibatkan buffer overflows.
2. Stack execute invalidation : Karena koding jahat (contoh, instruksi assembly untuk mengambil alih root shell) merupakan input argument ke dalam program, ini tersimpan ke dalam stack dan bukan dalam code segment. Oleh karena itu, solusi mudahnya adalah tidak mempebolehkan stack mengeksekusi instruksi apapun. Kode apapun yang dieksekusi dengan kode lainnya di dalam stack dapat mengakibatkan segmentation violation.
3. Compiler tools : Beberapa tahun terakhir, compiler mempunyai kemampuan lebih. Beberapa compiler dilengkapi peringatan dalam penggunakan konstruk yang tidak aman seperti gets(), strcpy() dan sejenisnya.

Daftar pustaka :

https://www.netcraft.com/

http://cve.mitre.org/cve/search_cve_list.html

https://logsmylife.wordpress.com/2009/03/31/konsep-buffer-overflow-vurnabilities-dan-pencegahannya/