МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет ім. М. Є. Жуковського

«Харківський авіаційний інститут»

Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій

Кафедра комп'ютерних систем, мереж і кібербезпеки

Практичне завдання №3

з дисципліни «Безпека індустріальних систем та Інтернету речей»

(назва дисципліни)

Виконав: студент 5 курсу групи № 555ім
напряму підготовки (спеціальності)
125 Кібербезпека та захист інформації

(шифр і назва напряму підготовки (спеціальності))

Орлов Станіслав Валерійович

(прізвище й ініціали студента)

Прийняв: доцент, кандидат технічних наук
Бабешко Євген Васильович

(посада, науковий ступінь, прізвище й ініціали)

Національна шкала: _____
Кількість балів: _____
Оцінка: ECTS _____

Харків – 2023

Ідентифікація компонентів

```
[    0.000000] 000: Booting Linux on physical CPU 0x0
[    0.000000] 000: Linux version 5.4.47-rt28-pxc (oe-user@oe-host) (gcc version 9.3.0 (GCC)) #1 SMP PREEMPT_RT Wed Dec 15 20:26:30 UTC 2021
[    0.000000] 000: CPU: ARMv7 Processor [412fc0f1] revision 1 (ARMv7), cr=30c5387d
[    0.000000] 000: CPU: div instructions available: patching division code
[    0.000000] 000: CPU: PIPT / VIPT nonaliasing data cache, PIPT instruction cache
[    0.000000] 000: OF: fdt: Machine model: linux,dummy-virt
[    0.000000] 000: Memory policy: Data cache writealloc
[    0.000000] 000: psci: probing for conduit method from DT.
[    0.000000] 000: psci: PSCIv0.2 detected in firmware.
[    0.000000] 000: psci: Using standard PSCI v0.2 function IDs
[    0.000000] 000: psci: Trusted OS migration not required
[    0.000000] 000: percpu: Embedded 15 pages/cpu s30496 r8192 d22752 u61440
[    0.000000] 000: Built 1 zonelists, mobility grouping on.  Total pages: 129536
[    0.000000] 000: Kernel command line: root=/dev/vda rw highres=off ip=dhcp console=ttyAMA0,115200
[    0.000000] 000: Dentry cache hash table entries: 65536 (order: 7, 524288 bytes, linear)
[    0.000000] 000: Inode-cache hash table entries: 32768 (order: 5, 131072 bytes, linear)
[    0.000000] 000: mem auto-init: stack:off, heap alloc:off, heap free:off
[    0.000000] 000: software IO TLB: mapped [mem 0x5b934000-0x5f934000] (64MB)
[    0.000000] 000: Memory: 435056K/524288K available (10240K kernel code, 658K rwdata, 1888K rodata, 2048K init, 320K bss, 89232K reserved, 0K cma-reserved
, 0K highmem)
[    0.000000] 000: SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=2, Nodes=1
[    0.000000] 000: ftrace: allocating 28933 entries in 57 pages
[    0.000000] 000: rcu: Preemptible hierarchical RCU implementation.
[    0.000000] 000: rcu:        RCU restricting CPUs from NR_CPUS=8 to nr_cpu_ids=2.
[    0.000000] 000: rcu:        RCU priority boosting: priority 1 delay 500 ms.
[    0.000000] 000: rcu:        RCU_SOFTIRQ processing moved to rcuc kthreads.
[    0.000000] 000:     No expedited grace period (rcu_normal_after_boot).
[    0.000000] 000:     Tasks RCU enabled.
[    0.000000] 000: rcu: RCU calculated value of scheduler-enlistment delay is 10 jiffies.
[    0.000000] 000: rcu: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=2
[    0.000000] 000: NR_IRQS: 16, nr_irqs: 16, preallocated irqs: 16
[    0.000000] 000: GICv2m: range[mem 0x08020000-0x08020fff], SPI[80:143]
[    0.000000] 000: random: get_random_bytes called from start_kernel+0x348/0x518 with crng_init=0
[    0.000000] 000: arch_timer: cp15 timer(s) running at 62.50MHz (virt).
[    0.000000] 000: clocksource: arch_sys_counter: mask: 0xffffffffffffff max_cycles: 0x1cd42e208c, max_idle_ns: 881590405314 ns
[    0.000124] 000: sched_clock: 56 bits at 62MHz, resolution 16ns, wraps every 4398046511096ns
[    0.000242] 000: Switching to timer-based delay loop, resolution 16ns
```

Підключення по SSH

```
PS C:\Users\sorlo> ssh admin@192.168.0.105 -p 5555
The authenticity of host '[192.168.0.105]:5555 ([192.168.0.105]:5555)' can't be established.
ED25519 key fingerprint is SHA256:yet8GUdrycqLJewy9iPqtMfMTiJxkEOE1OiTXpZ2Ps4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.105]:5555' (ED25519) to the list of known hosts.
Wichtiger Hinweis zur Verwendung der Simulation:
Die Simulation hat gegenüber dem realen Artikel Abweichungen
in Bezug auf Performance, Jitter und Funktion.
Dadurch kann ein simuliertes Projekt Abweichungen
im Vergleich zur realen Applikation haben.
Details hierzu sind in der Dokumentation aufgeführt.
Durch die weitere Verwendung der Simulation
erklären Sie sich mit diesen Bedingungen einverstanden.

Important note on the use of the simulation:
The simulation has deviations compared to the real article
in terms of performance, jitter and function.
Therefore a simulated project can have deviations
compared to the real application.
Details are listed in the documentation.
By continuing to use this simulation, you agree to these terms.admin@192.168.0.105's password:
Permission denied, please try again.
admin@192.168.0.105's password:
```

Username: admin
Password: plcnext

OpenSSL

Ідентифікація версії openssl

```
admin@192.168.0.105's password:
admin@sim-axcf1152:~$ openssl version
OpenSSL 1.1.1l  24 Aug 2021
admin@sim-axcf1152:~$
```

База даних вразливостей **CVEDetails** (https://www.cvedetails.com/)

https://www.cvedetails.com/version/681123/Openssl-Openssl-1.1.1l.html

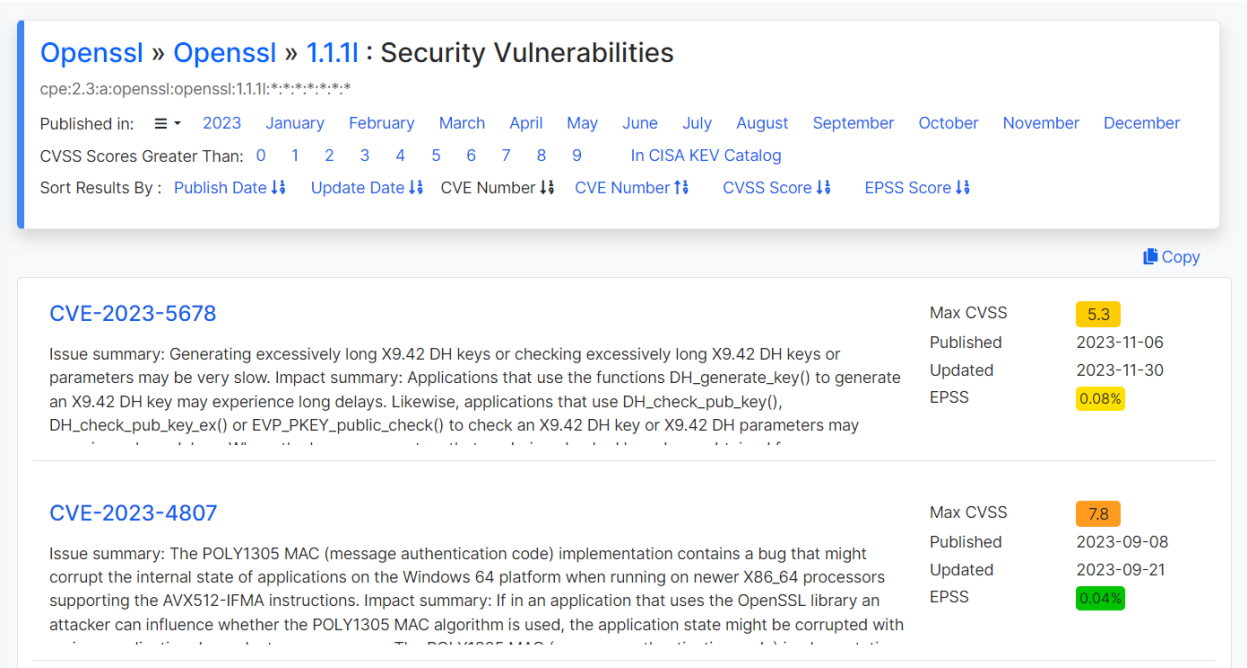

Рисунок 1 - База даних вразливостей CVEDetails

CVE-2023-4807

Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with

Max CVSS	7.8
Published	2023-09-08
Updated	2023-09-21
EPSS	0.04%

CVE-2023-3817

Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on

Max CVSS	5.3
Published	2023-07-31
Updated	2023-11-06
EPSS	0.13%

CVE-2023-2650

Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a

Max CVSS	6.5
Published	2023-05-30
Updated	2023-10-27
EPSS	0.14%

CVE-2023-0466

The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the

Max CVSS	5.3
Published	2023-03-28
Updated	2023-09-28
EPSS	0.13%

Рисунок 2 - Перегляд уразливостей через каталог уразливостей CVE (https://www.cve.org/)

CVE-2023-5678 Find

Find CVE Records by keyword.

website! CVE Records have a new and enhanced **format.** View records in the new format using the CVE ID lookup ab
ge. **CVE List keyword search** will be temporarily hosted on the legacy **cve.mitre.org** website until the **transition**

CVE-2023-5678 PUBLISHED

View JSON

Excessive time spent in DH check / generation with large Q parameter value

Important CVE JSON 5 Information +

Assigner: OpenSSL Software Foundation
Published: 2023-11-06 **Updated:** 2023-11-07

Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q.

Рисунок 3 – База даних вразливостей CVEDetails

CVE-2023-4807 Find

Find CVE Records by keyword.

ebsite! CVE Records have a new and enhanced format. View records in the new format using the CVE ID look
. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the trans

CVE-2023-4807 PUBLISHED

View JSON

POLY1305 MAC implementation corrupts XMM registers on Windows

Important CVE JSON 5 Information +

Assigner: OpenSSL Software Foundation
Published: 2023-09-08 **Updated:** 2023-09-12

Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind

Рисунок 4 - База даних вразливостей CVEDetails

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2023-5678
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2023-5678	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. **Published:** November 06, 2023; 11:15:42 AM -0500	*V3.1:* 5.3 MEDIUM *V2.0:*(not available)

Рисунок 5 – База даних вразливостей https://nvd.nist.gov/

EXPLOIT DATABASE

Verified Has App

Filters Reset All

Show 15

Search: openssl 1.1.

Date	D	A	V	Title	Type	Platform	Author
2017-01-26				OpenSSL 1.1.0 - Remote Client Denial of Service	DoS	Multiple	Guido Vranken
2016-12-11				OpenSSL 1.1.0a/1.1.0b - Denial of Service	DoS	Linux	Silverfox

Showing 1 to 2 of 2 entries (filtered from 45,784 total entries)

FIRST PREVIOUS 1 NEXT LAST

Рисунок 6 – база даних https://www.exploit-db.com/

Linux

https://www.cvedetails.com/version/1187513/Linux-Linux-Kernel-5.4.47.html

Ідентифікація версії Linux

```
0.000000] 000: Booting Linux on physical CPU 0x0
0.000000] 000: Linux version 5.4.47-rt28-pxc (oe-user@oe-host) (gcc version 9.3.0 (GCC)) #1 SMP PREEMPT_RT Wed Dec 15 20:26:30 UTC 2021
```

Linux » Linux Kernel » 5.4.47 (Operating system)

Vulnerabilities (**622**) Metasploit Modules

- Linux Kernel 5.4.47
- cpe:2.3:o:linux:linux_kernel:5.4.47:*:*:*:*:*:*:*
- cpe:/o:linux:linux_kernel:5.4.47

Vulnerability trends over time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2017		1									
2019		1									
2020	5	26			1						2
2021	16	37			2						4
2022	26	112									1
2023	9	116									1
Total	56	293			3						8

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2017				1	
2019				2	
2020			2	13	2
2021	4	1	2	18	3
2022	6	9	11	35	16
2023	9	1	27	30	6
Total	19	11	42	99	27

CVE-2023-6622 Find

Find CVE Records by keyword.

a website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above
age. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition is c

CVE-2023-6622 PUBLISHED

View JSON

Kernel: null pointer dereference vulnerability in nft_dynset_init()

Important CVE JSON 5 Information +

Assigner: Red Hat, Inc.
Published: 2023-12-08 **Updated:** 2023-12-08

A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CAP_NET_ADMIN user privilege to trigger a denial of service.

Product Status

CVE-2023-6560 Find

Find CVE Records by keyword.

website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup abo
e. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition i

CVE-2023-6560 PUBLISHED

View JSON

Kernel: io_uring out of boundary memory access in __io_uaddr_map()

Important CVE JSON 5 Information +

Assigner: Red Hat, Inc.
Published: 2023-12-08 **Updated:** 2023-12-08

An out-of-bounds memory access flaw was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue could allow a local user to crash the system.

Product Status

Learn About the Versions Section +

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2023-6622
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2023-6622	A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CAP_NET_ADMIN user privilege to trigger a denial of service. **Published:** December 08, 2023; 1:15:07 PM -0500	*V3.1:* 5.5 MEDIUM *V2.0:*(not available)

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2023-6650
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2023-6650	A vulnerability was found in SourceCodester Simple Invoice Generator System 1.0 and classified as problematic. This issue affects some unknown processing of the file login.php. The manipulation of the argument cashier leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-247343. **Published:** December 10, 2023; 6:15:07 AM -0500	*V3.1:* 6.1 MEDIUM *V2.0:*(not available)

EXPLOIT DATABASE

Verified Has App

Filters Reset All

Show 15

Search: linux kernel 5.4

Date	D	A	V	Title	Type	Platform	Author
2021-04-08				Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution	Remote	Linux	Google Security Research
2018-03-22				Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak	Local	Linux	Gregory Draperi

Showing 1 to 2 of 2 entries (filtered from 45,784 total entries)

FIRST PREVIOUS 1 NEXT LAST

EXPLOIT DATABASE

Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49754	2020-12352 2020-12351	GOOGLE SECURITY RESEARCH	REMOTE	LINUX	2021-04-08

EDB Verified: ✕

Exploit: / {}

Vulnerable App:

Nginx

```
admin@sim-axcf1152:~$ nginx -v
nginx version: nginx/1.16.1
admin@sim-axcf1152:~$
```

CVEdetails.com
powered by SecurityScorecard

Vulnerabilities
By Date
By Type
Known Exploited
Assigners
CVSS Scores
EPSS Scores
Search

Vulnerable Software
Vendors
Products

F5 » Nginx » 1.16.1

Vulnerabilities (**4**) Metasploit Modules

- F5 NGINX 1.16.1
- cpe:2.3:a:f5:nginx:1.16.1:*:*:*:*:*:*:*
- cpe:/a:f5:nginx:1.16.1

Product information

https://www.f5.com/products/nginx Product

https://www.f5.com/ Vendor

https://github.com/nginx/nginx Version

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2020					
2021					
2022					
2023				1	
Total				1	

F5 » Nginx » 1.16.1 : Security Vulnerabilities Published In 2023 (Denial of service)

cpe:2.3:a:f5:nginx:1.16.1:*:*:*:*:*:*:*

Published in: 2023 January February March April May June July August September October November December

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2023-44487

Known Exploited Vulnerability

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Max CVSS	7.5
Published	2023-10-10
Updated	2023-12-20
EPSS	64.49%
KEV Added	2023-10-10

Vulnerability Details : CVE-2023-44487

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Vulnerability category: Denial of service

Published 2023-10-10 14:15:11 Updated 2023-12-20 17:55:37 Source MITRE

View at NVD, CVE.org

CVE-2023-44487 is in the CISA Known Exploited Vulnerabilities Catalog

CISA vulnerability name:
HTTP/2 Rapid Reset Attack Vulnerability

CISA required action:
Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

CISA description:
HTTP/2 contains a rapid reset vulnerability that allows for a distributed denial-of-service attack (DDoS).

Notes:
https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/

Added on 2023-10-10 Action due date 2023-10-31

CVE About Partner Information Program Organization Downloads Resources & Support Report/Request

CVE-2023-44487 Find

Find CVE Records by keyword.

Site Search

Welcome to the new CVE Beta website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above or download them on the Downloads page. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition is complete.

CVE-2023-44487 PUBLISHED

View JSON

Important CVE JSON 5 Information +

Assigner: MITRE Corporation
Published: 2023-10-10 **Updated:** 2023-12-02

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Product Status

Learn About the Versions Section +

References

- https://github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/release-notes/6.0/6.0.23/6.0.23.md?plain=1#L73
- https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/
- https://aws.amazon.com/security/security-bulletins/AWS-2023-011/
- https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
- https://www.nginx.com/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products/
- https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/
- https://news.ycombinator.com/item?id=37831062
- https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/
- https://www.phoronix.com/news/HTTP2-Rapid-Reset-Attack
- https://github.com/envoyproxy/envoy/pull/30055
- https://github.com/haproxy/haproxy/issues/2312
- https://github.com/eclipse/jetty.project/issues/10679
- https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764
- https://github.com/nghttp2/nghttp2/pull/1961
- https://github.com/netty/netty/commit/58f75f665aa81a8cbcf6ffa74820042a285c5e61
- https://github.com/alibaba/tengine/issues/1872
- https://github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES | SEARCH AND STATISTICS

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2023-44487
- Search Type: Search All
- Match: Exact
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2023-44487	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. **Published:** October 10, 2023; 10:15:10 AM -0400	*V3.1:* 7.5 HIGH *V2.0:*(not available)

CVE-2023-44487 Detail

Description

The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

EXPLOIT DATABASE

Verified Has App

Filters Reset All

Show 15

Search: nginx 1.16.1

Date	D	A	V	Title	Type	Platform	Author
No matching records found							

Showing 0 to 0 of 0 entries (filtered from 45,784 total entries)

FIRST PREVIOUS NEXT LAST