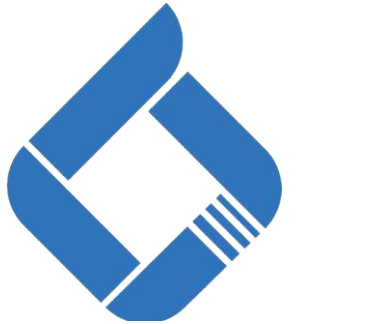
مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه‌ای



مرکز تخصصی آیا
دانشگاه مازندران

شناسایی، جمع‌آوری و تحلیل آسیب‌پذیری‌های سازمانی

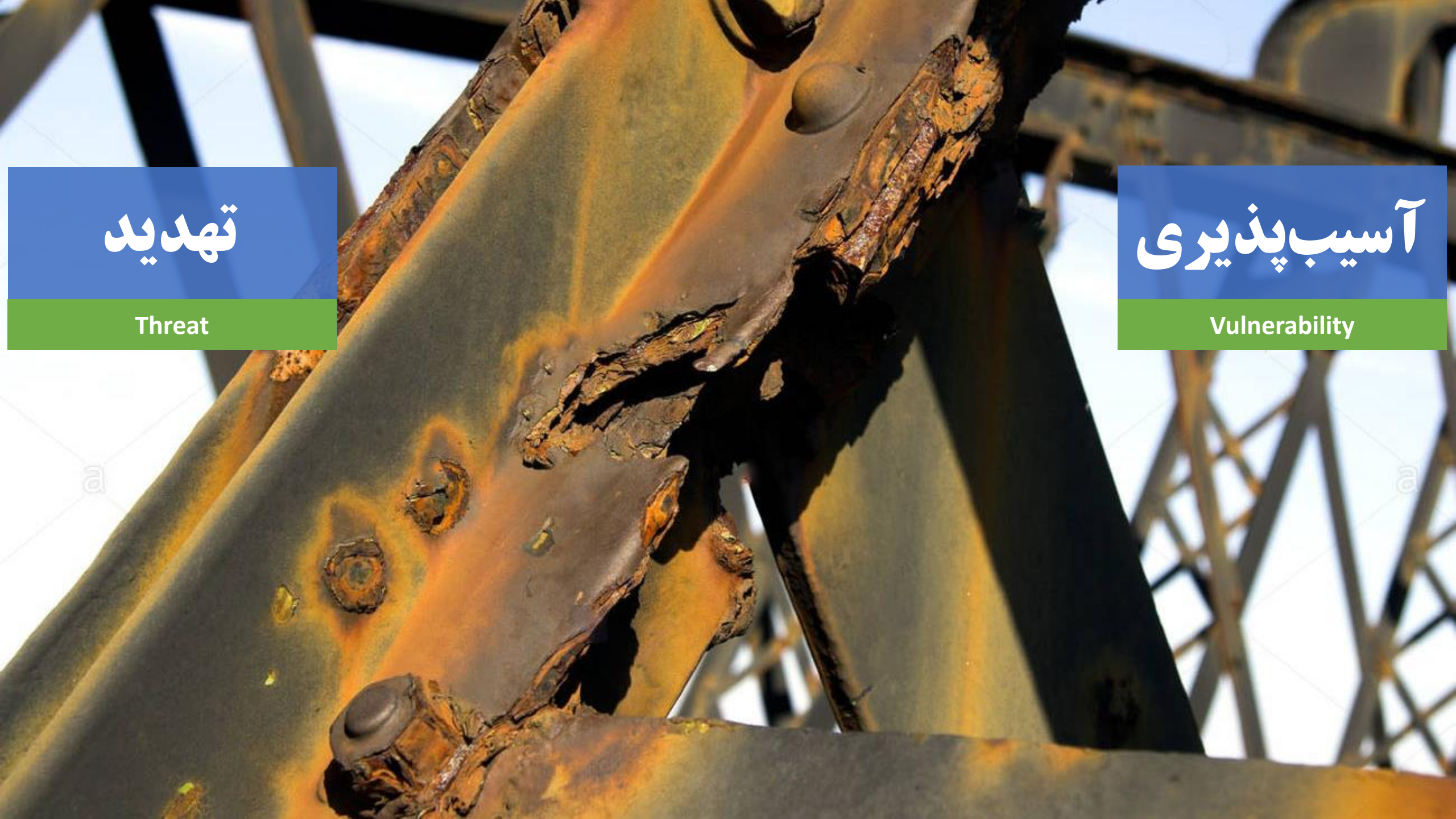
شهریور ۱۴۰۲

مرکز تخصصی آیا
دانشگاه مازندران

تعاریف

Vulnerability

- **آسیب‌پذیری:** به ضعف یا نقصی در سیستم، نرم‌افزار، شبکه یا فرآیند اشاره دارد که می‌تواند توسط یک حمله‌کننده برای نقض محرمانگی، صحت یا دسترسی سیستم یا داده‌های آن بهره‌برداری شود.
- **تهدید:** تهدید به خطر وقوع یا رویداد مضر اشاره دارد که می‌تواند از طریق آسیب‌پذیری‌ها به امنیت یک سیستم یا سازمان آسیب برساند.
- **حمله:** حمله به عملیاتی تعمدی و بدخواهانه اشاره دارد که توسط یک فرد، گروه یا سیستم خودکار برای بهره‌برداری از آسیب‌پذیری‌ها و نقض امنیت یک سیستم هدف یا سازمان انجام می‌شود. حملات قصد دارند صدمه‌ای وارد کنند، دسترسی غیرمجاز را به دست آورند، اطلاعات حساس را دزدیده، عملکرد را مختل کنند یا سیستم‌ها را برای اهداف شرورانه تغییر دهند.


تهدید
Threat
آسیب‌پذیری
Vulnerability

رخداد امنیتی

Incident or Loss

مرکز تخصصی آیا
دانشگاه مازندران

آسیب‌پذیری روز صفر

Zero Days or 0-days

Zero Day

مرکز تخصصی آیا
دانشگاه مازندران

آسیب‌پذیری روز صفر

Zero Days or 0-days

- **آسیب‌پذیری روز صفر:** یک آسیب‌پذیری یا نقص امنیتی در یک سیستم نرم‌افزاری یا سخت‌افزاری است که برای تولید کننده و یا جامعه امنیتی هنوز شناخته شده نیست.

- عبارت **"صفر روز"** اشاره به آن دارد که تولید کننده، صفر روز برای رفع یا پچ کردن آسیب‌پذیری قبل از آنکه توسط حمله‌کنندگان مورد بهره‌برداری قرار گیرد، زمان داشته است.

- به عبارت دیگر، این یک آسیب‌پذیری است که به صورت فعال توسط عاملان خرابکار معمولاً قبل از ارائه پچ یا مکانیزم مرتفع سازی، بهره‌برداری می‌شود.

مکانیزم‌های مقابله با آسیب‌پذیرهای روزصفر

Zero Days or 0-days

- Stay Updated
- Implement Defense-in-Depth
- Network Segmentation
- Application Whitelisting:
- Deploy IDS and IPS solutions
- Participate in bug bounty programs
- …

مرکز تخصصی آیا
دانشگاه مازندران

جایزه بگیر

Bug Bounty

Common Vulnerabilities and Exposures

شناسه آسیب‌پذیری

مرکز تخصصی آیا

دانشگاه مازندران

CVE چیست؟

- CVE (Common Vulnerabilities and Exposures) همان آسیب‌پذیری‌ها و افشاعات امنیتی عمومی شده است.
- یک سیستم و استاندارد که برای شناسایی و پیگیری آسیب‌پذیری‌های عمومی شده در نرم‌افزارها و سخت‌افزارها استفاده می‌شود.
- هر ورودی CVE یک شناسه یکتا دارد، مانند " "CVE-2021-12345که برای ارجاع به یک آسیب‌پذیری خاص استفاده می‌شود.
- پژوهشگران امنیتی، متخصصان و سازمان‌ها می‌توانند آسیب‌پذیری‌ها را به سیستم CVE ارسال کنند، که سپس شناسه‌های یکتا به آنها اختصاص داده و به صورت عمومی قابل دسترسی می‌شوند.

مرکز تخصصی آیا
دانشگاه مازندران

شناسنامه آسیب‌پذیری

Common Vulnerabilities and Exposures

در سال ۱۹۹۹ شرکت مایتر پیشنهاد کرد تا هر آسیب‌پذیری یک شناسنامه شامل جزئیات و شرح آسیب پذیری، درجه‌ی اهمیت، اصلاحیه‌های تکمیلی و روش‌های کاهش تهدید مربوط به آن آسیب‌پذیری و ... در گزارشی با شناسه CVE منحصر به فرد، داشته باشد.

مرکز تخصصی آیا
دانشگاه مازندران

شناسه آسیب‌پذیری

Common Vulnerabilities and Exposures

شناسه‌ای برای آدرس‌دهی آسیب‌پذیری‌ها و افشاعات امنیتی عمومی شده است.

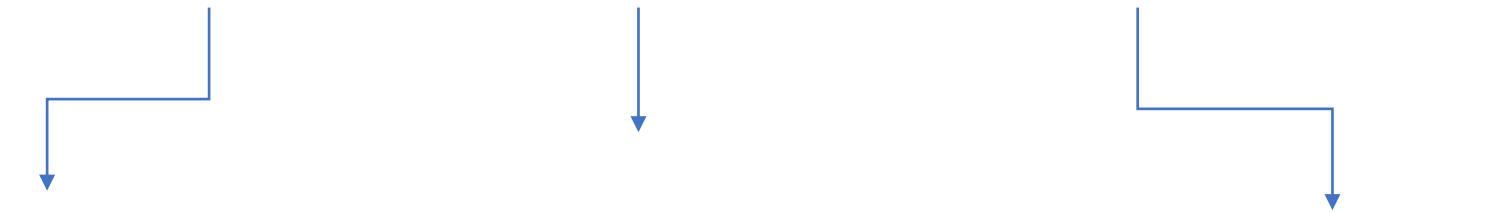
- این پروژه توسط شرکت MITRE پایه ریزی شد که بعدها مورد حمایت سازمان امنیت ملی آمریکا قرار گرفت.
- اطلاعات این پروژه از سال ۱۹۹۹ برای عموم در دسترس است.

CVE-2020-25824

CVE ID

Common Vulnerabilities and Exposures

CVE-2020-25824



CVE Format

Common Vulnerabilities and Exposures

CVE - CVE-2020-25824

cve.mitre.org/cgi-bin/cvename.cgi?name=C

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD Go to for: CVSS Scores CPE Info

Full-Screen View

CVE-ID	
CVE-2020-25824	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has voluntarily opened Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chat conversation and media files.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- GENTOO:GLSA-202101-34
- URL:https://security.gentoo.org/glsa/202101-34
- MISC:https://github.com/soheilsamanabadi/vulnerability/blob/main/Telegram-Desktop-CVE-2020-25824
- MISC:https://github.com/telegramdesktop/tdesktop/releases/tag/v2.4.3
- MISC:https://www.Telegram.org

Assigning CNA

MITRE Corporation

Date Record Created

20200923	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200923)

Votes (Legacy)

Comments (Legacy)

CVE Format

Common Vulnerabilities and Exposures

CVE - CVE-2020-25824

cve.mitre.org/cgi-bin/cvename.cgi?name=C

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Full-Screen View

CVE-ID	
CVE-2020-25824	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has voluntarily opened Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chat conversation and media files.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- GENTOO:GLSA-202101-34
- URL:https://security.gentoo.org/glsa/202101-34
- MISC:https://github.com/soheilsamanabadi/vulnerability/blob/main/Telegram-Desktop-CVE-2020-25824
- MISC:https://github.com/telegramdesktop/tdesktop/releases/tag/v2.4.3
- MISC:https://www.Telegram.org

شماره یکتای آسیب‌پذیری

CVE ID

Assigning CNA

MITRE Corporation

Date Record Created

20200923	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200923)

Votes (Legacy)

Comments (Legacy)

CVE Format

Common Vulnerabilities and Exposures

CVE - CVE-2020-25824

cve.mitre.org/cgi-bin/cvename.cgi?name=C

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD
Go to for:
CVSS Scores
CPE Info

Full-Screen View

CVE-ID

CVE-2020-25824 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has voluntarily opened Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chat conversation and media files.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- GENTOO:GLSA-202101-34
- URL:https://security.gentoo.org/glsa/202101-34
- MISC:https://github.com/soheilsamanabadi/vulnerability/blob/main/Telegram-Desktop-CVE-2020-25824
- MISC:https://desktop.telegram.org/changelog#2-4-4-beta
- MISC:https://www.Telegram.org

Assigning CNA

MITRE Corporation

Date Record Created

20200923 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200923)

Votes (Legacy)

Comments (Legacy)

<Problem> in <Version> of <Product> result in <Impact> when exposed to <Attack>

توضیحات تکمیلی

Description

CVE Format

Common Vulnerabilities and Exposures

CVE - CVE-2020-25824

cve.mitre.org/cgi-bin/cvename.cgi?name=C

CVE List • CNAs • WGs • Board • About • News & Blog

NVD Go to for: CVSS Scores CPE Info

Full-Screen View

CVE-ID

CVE-2020-25824 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

ارجاع‌ها

References

Description

Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has [illegible] Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chats, contacts, and media files.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- GENTOO:GLSA-202101-34
- URL:https://security.gentoo.org/glsa/202101-34
- MISC:https://github.com/soheilsamanabadi/vulnerability/blob/main/Telegram-Desktop-CVE-2020-25824
- MISC:https://github.com/telegramdesktop/tdesktop/releases/tag/v2.4.3
- MISC:https://www.Telegram.org

Assigning CNA

MITRE Corporation

Date Record Created

20200923 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200923)

Votes (Legacy)

Comments (Legacy)

CVE Format

Common Vulnerabilities and Exposures

CVE - CVE-2020-25824

cve.mitre.org/cgi-bin/cvename.cgi?name=C

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾ News & Blog ▾

NVD Go to for: CVSS Scores CPE Info

Full-Screen View

CVE-ID

CVE-2020-25824 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Telegram Desktop through 2.4.3 does not require passcode entry upon pushing the Export key within the Export Telegram Data wizard. The threat model is a victim who has voluntarily opened Export Wizard but is then distracted. An attacker then approaches the unattended desktop and pushes the Export key. This attacker may consequently gain access to all chat conversation and media files.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- GENTOO:GLSA-202101-34
- URL:https://security.gentoo.org/glsa/202101-34
- MISC:https://github.com/soheilsamanabadi/vulnerability/blob/main/Telegram-Desktop-CVE-2020-25824
- MISC:https://github.com/telegramdesktop/tdesktop/releases/tag/v2.4.3
- MISC:https://www.Telegram.org

Assigning CNA

MITRE Corporation

Date Record Created

20200923 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200923)

Votes (Legacy)

Comments (Legacy)

NATIONAL VULNERABILITY DATABASE

NVD

- موسسه ملی استاندارد و فناوری آمریکا بررسی درجه اهمیت آسیب‌پذیری‌ها را به مرجعی به نام NVD سپرده است.
- مهم‌ترین وظایف NVD شامل موارد زیر است:
  - تعیین سطح آسیب‌پذیری یا CVSS
  - تعیین دسته بندی ضعف موجود در محصول یا CWE
  - مشخص کردن محصولات تحت تاثیر این آسیب‌پذیری یا CPE

درجه آسیب‌پذیری

Scoring

آسیب‌پذیری حیاتی Netlogon

CVE-2020-1472

NVD - cve-2020-1472

nvd.nist.gov/vuln/detail/cve-2020-1472

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

CVE-2020-1472 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

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

+View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2020-1472
NVD Published Date:
08/17/2020
NVD Last Modified:
12/24/2020
Source:
Microsoft Corporation

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

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

Link:
https://nvd.nist.gov/vuln/detail/cve-2020-1472

درجه آسیب‌پذیری

Common Vulnerability Scoring System

- سنجش شدت آسیب‌پذیری‌ها بر اساس استاندارد **CVSS** تخمین زده می‌شود.

CVSS v2.0 Ratings

Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

محاسبه شدت آسیب‌پذیری

Common Vulnerability Scoring System

شاخص‌های اندازه‌گیری CVSS v3

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

قابلیت بهره‌برداری

بردار حمله Attack Vector (AV)

Network (N) شبکه | Adjacent (A) مجاورت

پیچیدگی حمله Attack Complexity (AC)

Low (L) کم | High(H) زیاد

اجازه دسترسی Privilege Required (PR)

None(N) نیاز ندارد | Low (L) کم | High(H) زیاد

تعامل کاربر User Interaction (UI)

None(N) نیاز ندارد | Requierd (R) نیاز دارد

محدوده

محدوده اثرگذاری Scope (S)

Changed (C) تغییریافته | Unchanged (U) بدون تغییر

شدت اثرگذاری محرمانگی Confidentiality Impact (C)

High(H) زیاد | Low (L) کم | None (N) بی‌تاثیر

شدت اثرگذاری یکپارچگی Integrity Impact (I)

High(H) زیاد | Low (L) کم | None (N) بی‌تاثیر

شدت اثرگذاری دسترسی‌پذیری Availability (A)

High(H) زیاد | Low (L) کم | None (N) بی‌تاثیر

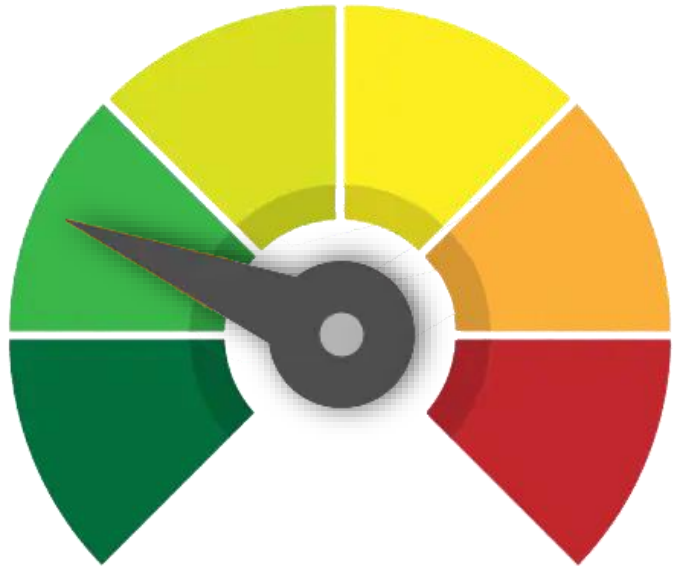
خطرناک‌ترین آسیب‌پذیری‌های سوء استفاده شده در ایران

Recent high-impact CVES

PrintNightmare
CVE-2021-1675

BLUEKEEP
CVE-2019-0708

EternalBlue
CVE-2017-0144



MS Exchange
CVE-2021-27065

Zerologon
CVE-2020-1472

Shellshock
CVE-2014-6271

STUXNET
CVE-2010-2772
CVSS: 6.9

Sunburst
CVE-2021-25275
CVSS v3: 7.8

در طرح غربالگری اقدام‌های امنیتی دستگاه‌های استان مازندران، از میان ۲۰ سازمان بازدید شده تا تاریخ ۲۰ شهریور۱۴۰۲، فقط **یک** کارشناس فناوری اطلاعات با مفهوم آسیب‌پذیری که در بند ۱۶ فرم غربالگری ذکر شده است آشنایی داشته است.

خطرناک‌ترین آسیب‌پذیری‌ها

https://www.cvedetails.com/

CVE security vulnerability databa

cvedetails.com

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search

View CVE

Log In Register

Vulnerability Feeds & Widgets New

www.itsecdb.com

Switch to https://

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Click Here!

Search

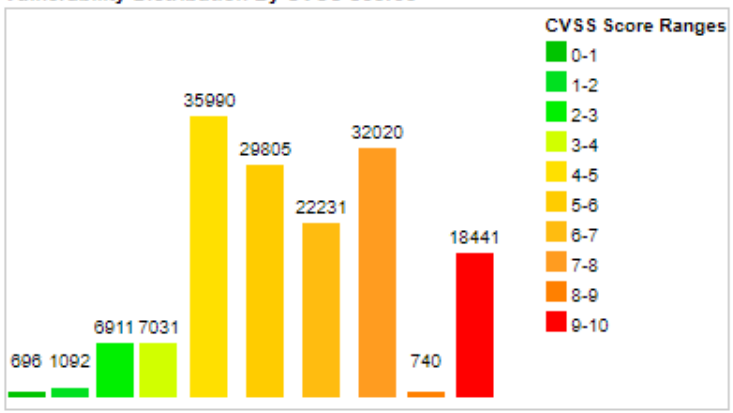
Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	696	0.40
1-2	1092	0.70
2-3	6911	4.50
3-4	7031	4.50
4-5	35990	23.20
5-6	29805	19.20
6-7	22231	14.30
7-8	32020	20.70
8-9	740	0.50
9-10	18441	11.90
Total	154957	

Weighted Average CVSS Score: **6.5**

Vulnerability Distribution By CVSS Scores



Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.

Sample CVE entry with OVAL definitions : CVE-2007-0994

پایگاه اطلاعاتی CVE Details منبعی برای دستیابی به دسته‌بندی‌های متنوع از آسیب‌پذیری‌های لیست شده است.

شناسه ضعف کدنویسی

Common Weakness Enumeration

CWE

Common Weakness Enumeration

A Community-Developed List of Software Weakness Types

برای مثال: آسیب‌پذیری کشف شده در تلگرام با شناسه CVE-2020-25824 در اثر ضعف کدنویسی CWE-862 به وجود آمده است.

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-862	Missing Authorization	NIST

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
[11]	CWE-190	Integer Overflow or Wraparound	15.81
[12]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67
[13]	CWE-476	NULL Pointer Dereference	8.35
[14]	CWE-287	Improper Authentication	8.17
[15]	CWE-434	Unrestricted Upload of File with Dangerous Type	7.38
[16]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.95
[17]	CWE-94	Improper Control of Generation of Code ('Code Injection')	6.53
[18]	CWE-522	Insufficiently Protected Credentials	5.49
[19]	CWE-611	Improper Restriction of XML External Entity Reference	5.33
[20]	CWE-798	Use of Hard-coded Credentials	5.19
[21]	CWE-502	Deserialization of Untrusted Data	4.93
[22]	CWE-269	Improper Privilege Management	4.87
[23]	CWE-400	Uncontrolled Resource Consumption	4.14
[24]	CWE-306	Missing Authentication for Critical Function	3.85
[25]	CWE-862	Missing Authorization	3.77

CWE Top 25 Most Dangerous Software Errors

Common Weakness Enumeration

CWE vs. CVE

Common Weakness Enumeration

- CWE is a comprehensive catalog of software weaknesses, while CVE is a database of specific vulnerabilities that have been reported and assigned unique identifiers.
- CWE focuses on categorizing and describing different types of weaknesses, whereas CVE focuses on tracking and providing information about known vulnerabilities.
- Both frameworks are valuable resources for understanding, addressing, and mitigating software security issues.

مراحل گزارش آسیب‌پذیری

The process of registering a CVE:

1. **Discovery of Vulnerability**: A security researcher, organization, or vendor identifies a vulnerability in software or hardware through security testing, code analysis, or incident response.
2. **Vulnerability Reporting**: The discovered vulnerability is reported to the relevant vendor or organization responsible for maintaining the affected product. The report should include detailed information about the vulnerability, its potential impact, and any supporting evidence.
3. **Vendor Confirmation and Analysis**: The vendor acknowledges the vulnerability report and initiates an investigation. They verify the reported vulnerability and assess its severity and potential impact on their product or system.
4. **CVE Assignment**: If the vendor confirms the vulnerability and determines it to be a valid security issue, they may request a CVE identifier from the CVE Numbering Authority (CNA) or directly register it themselves. The CVE identifier is a unique identifier used to reference the vulnerability.
5. **Coordination and Disclosure**: The vendor, in coordination with the CNA or responsible disclosure guidelines, establishes a timeline and plan for fixing the vulnerability and releasing a security patch or update. They may also collaborate with the security researcher who discovered the vulnerability to ensure accurate and timely disclosure.
6. **Vulnerability Mitigation**: The vendor develops a fix or workaround to address the vulnerability. This may involve patching the affected software, updating firmware, or implementing other mitigating measures to eliminate or reduce the vulnerability's impact.
7. **Patch Release and Communication**: The vendor releases the security patch or update to the affected users or customers. They communicate the availability of the fix, along with instructions on how to apply it, to ensure users can protect their systems and mitigate the risk.
8. **Public Disclosure**: Once the patch is available and users have had sufficient time to apply it, the vendor and/or the CNA publicly disclose the vulnerability, including the CVE identifier, a description of the vulnerability, and information on how to mitigate it. This promotes transparency and allows the broader security community to be aware of the vulnerability.

نحوه بهره‌برداری از شناسه آسیب‌پذیری

using and addressing CVEs

OpenCVE
CVE Alerting Platform

INTERNET STORM CENTER

SHODAN
Computer Search Engine

Nessus™

1. **Stay Informed:** Stay updated on the latest CVEs by following trusted sources of information such as security advisories, vulnerability databases, and official announcements from software vendors, security organizations, and your national Computer Emergency Response Team (CERT).
2. **Assess Impact:** Understand the impact of a CVE on your systems or organization. Evaluate the severity, potential attack vectors, and the assets or software that may be affected. This assessment helps in prioritizing your response efforts.
3. **Vulnerability Management**: Implement a vulnerability management program that includes scanning and assessing your systems for known vulnerabilities, including those identified by CVEs. Utilize automated tools or services to identify and track vulnerabilities in your environment.
4. **Patch Management**: Apply patches and updates provided by software vendors to address the vulnerabilities associated with CVEs. Prioritize critical and high-severity patches and ensure a timely deployment process to minimize exposure.
5. **Mitigation and Workarounds**: In cases where patches are not immediately available, consider implementing temporary mitigations or workarounds to reduce the risk associated with the CVE. This might involve applying configuration changes, disabling affected features, or implementing additional security controls.
6. **Incident Response**: Include CVEs as part of your incident response plan. Establish procedures to detect, respond, and recover from incidents related to known vulnerabilities. This includes monitoring for any signs of exploitation and taking appropriate actions to contain and mitigate any potential impact.
7. **Security Awareness and Training**: Educate your users and staff about the importance of CVEs, the risks associated with unpatched vulnerabilities, and how to report potential security issues. Encourage a culture of security awareness and proactive reporting.
8. **Continuous Monitoring**: Maintain ongoing monitoring and scanning of your systems for new

الزامات قانونی و تامین هزینه مرتبط با امنیت سایبری در قانون بودجه سال ۱۴۰۲

- **با توجه به بند س – تبصره ۱۹ قانون بودجه ۱۴۰۲ کشور**، از آنجایی که یکی از اولویت‌های برنامه اجرایی پدافند غیرعامل سال ۱۴۰۲، امن سازی مراکز داده در زیرساخت‌های حیاتی و حساس و مهم است. بر اساس دستورالعمل **اجرایی بند س تبصره ۱۹ قانون بودجه سال جاری،** شرکت‌های دولتی، بانک‌ها و موسسات انتفاعی وابسته به دولت و شرکت‌های دولتی که مشمول قانون بر آنها مستلزم ذکر یا تصریح نام است ملزم هستند **حداکثر یک درصد** از مصارف خود (هزینه‌ها و هزینه‌های سرمایه‌ای) و دستگاه های اجرایی دارای اعتبار در جدول شماره ۷ این قانون نیز **حداکثر یک درصد** از اعتبارات تملک دارایی‌های سرمایه‌ای ابلاغی خود **را بر اساس اعلام سازمان پدافند غیرعامل مبنی بر الزامی بودن هزینه‌کرد، در زیرساخت‌های حیاتی، حساس و مهم خود هزینه نمایند**.

- **همچنین با توجه به بند ز- تبصره ۷ قانون بودجه ۱۴۰۲**، تمام دستگاه های اجرایی موضوع ماده ۲۹ قانون پنج ساله ششم توسعه و شرکتهای دولتی و نهادها و سازمانهایی که از بودجه عمومی استفاده می‌کنند، مکلفند **یک تا دو درصد** از اعتبارات هزینه‌ای یا تملک دارایی سرمایه‌ای خود را برای **تضمین و ارتقای سطح امنیت شبکه، امنیت زیرساخت‌ها و امنیت سامانه های خود و پیشگیری موثر از وقوع حوادث امنیتی سایبری** در دستگاه خود اختصاص دهند. لذا جهت ارتقا امنیت سایبری دستگاه خود، با توجه به اینکه **مسئولیت تامین امنیت سایبری شبکه و سامانه های دستگاه های اجرایی برعهده بالاترین مقام دستگاه اجرایی است**، اهتمام به جذب و هزینه‌کرد اعتبارات مذکور در حوزه سایبری، مورد تاکید می‌باشد.

CNA

CVE Numbering Authority

- **The CVE Numbering Authority (CNA)** is an organization or entity responsible for assigning CVE identifiers to vulnerabilities. CNAs play a crucial role in the CVE ecosystem by ensuring the proper identification and tracking of vulnerabilities.

Here are some key points about CNAs:

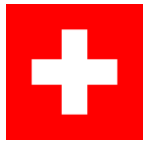
- **Role and Responsibilities**: CNAs act as the primary point of contact for receiving vulnerability reports, validating them, and assigning CVE identifiers. They are responsible for coordinating the vulnerability disclosure process, working with vendors, researchers, and the wider security community.
- **CVE Assignment**: CNAs follow the CVE program's guidelines and rules to assign unique CVE identifiers to reported vulnerabilities. They maintain a database of assigned CVEs and associated information.

Types of CNAs: There are two types of CNAs:

- a. **Primary (Root) CNAs**: Examples of primary CNAs include MITRE, which is the primary CVE Numbering Authority, and organizations like Microsoft and Red Hat.
- b. **Secondary CNAs**: These are organizations or entities that have been authorized by a primary CNA to assign CVEs within a **specific scope**, such as a particular software product or industry sector. Secondary CNAs help distribute the CVE assignment workload and cater to specific areas of focus.JPCERT/CC: The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) is a secondary **CNA responsible for assigning CVE identifiers to vulnerabilities related to Japanese software and systems**.

CNA

CVE Numbering Authority



NCSC
Switzerland

TWCERT/CC
Taiwan

KrCERT/CC
South Korea

TR-CERT
Türkiye

JPCERT/CC
Japan

GovTech CSG
Singapore

CERT-In
India

NCSC-FI
Finland

CERT.PL
Poland

NCSC-NL
Netherlands

INCIBE
Spain

SK-CERT
Slovak Republic

huntr.dev
UK

CERT@VDE
Germany

NVN

National Vulnerability Number

شناسه آسیب‌پذیری محصولات ایرانی

NVN

National Vulnerability Number

- طراحی یک سیستم برای گزارش و استعلام آسیب‌پذیری یک امر حیاتی در زمینه امنیت فناوری اطلاعات است. چنین سیستمی که نظیر بومی شده آن در کشور موجود نیست، علاوه بر اینکه کمک مبرمی به افزایش آگاهی افراد می‌کند، باعث افزایش چشمگیر امنیت در زیرساخت های کشور می‌گردد.

- این سیستم به تشخیص و پیگیری آسیب‌پذیری‌ها کمک می‌کند و در مدیریت امنیت سازمان‌ها و شبکه‌ها بسیار مؤثر و اساسی است.

- طراحی یک سیستم گزارش و استعلام آسیب‌پذیری، ابزاری اساسی برای مدیریت و بهبود امنیت اطلاعات و فناوری اطلاعات است. این سیستم به سازمان‌ها این امکان را می‌دهند که به صورت جدی‌تری به مسائل امنیتی پاسخ دهند و خطرات احتمالی را به حداقل برسانند.

NVN

National Vulnerability Number

NVN-402-25824

شناسه

سال انتشار

شماره اختصاصی

NVN-402-0001

شرح آسیب‌پذیری

ضعف سرریز بافر (Buffer overflow) در نسخه ۶.۰۱ نرم‌افزار روبیکا، موجب می‌شود مهاجم از راه دور با تزریق قطعه کد از طریق ارسال فایل آلوده به پیام‌ها دسترسی پیدا کند.

شدت آسیب‌پذیری

بحرانی

راهکار کاهش مخاطره

۱- غیرفعال نمودن قابلیت دانلود خودکار فایل‌ها در گروه‌ها
۲- به روز رسانی به نسخه ۶.۰۲ نرم‌افزار

سامانه‌های تحت تاثیر

Rubika 6.01 Android application

نهاد افشاء کننده

مرکز آپای دانشگاه مازندران

سطح دسترسی به محتوا:

استعلام عمومی

تاریخ ثبت

۱۱ مرداد ۱۴۰۲

کاربرد و مزایا

benefits

1. **تشخیص زودهنگام آسیب‌پذیری‌ها**: سیستم‌های گزارش و استعلام آسیب‌پذیری به سازمان‌ها این امکان را می‌دهند تا آسیب‌پذیری‌ها را در مراحل ابتدایی تشخیص داده و اقدامات لازم برای رفع یا محدود کردن تأثیر آسیب‌پذیری را انجام دهند.

2. **مدیریت و برنامه‌ریزی امنیتی**: سیستم گزارش و استعلام آسیب‌پذیری به اپراتورهای امنیتی و مدیران سازمان کمک می‌کند تا آسیب‌پذیری‌ها را با اولویت‌بندی صحیح مدیریت کنند و اقدامات مناسب برای تقویت امنیت را انجام دهند.
3. **جلوگیری از تکرار رویداد امنیتی گزارش شده**
4. **افزایش همکاری و اشتراک گذاری اطلاعات**: این سیستم‌ها به محققان امنیتی، توسعه‌دهندگان نرم‌افزار، و تیم‌های امنیتی در سازمان‌ها کمک می‌کنند تا اطلاعات در مورد آسیب‌پذیری‌ها را به صورت جامع و هماهنگ به اشتراک بگذارند.

5. **پایش و ارزیابی مداوم:** این سیستم به سازمان‌ها امکان می‌دهند تا آسیب‌پذیری‌ها را به طور مداوم پایش کرده و ارزیابی امنیت خود را بهبود بخشند.

چالش‌ها

Challenges

عدم پیروی شرکت‌های نرم‌افزاری از استانداردهای تعیین نسخه

چالش‌ها

Challenges

عدم همکاری شرکت‌های اعطا کننده گواهی ارزیابی امنیتی

چالش‌ها

Challenges

رویکرد مراجع امنیتی نسبت به عدم افشای آسیب‌پذیری‌ها به صورت عمومی