CVE Advisories

CVE Advisories

Open All Close All

All Vulnerabilities

ILVN-ID	Title	CVE-ID	Date
ILVN-2022-0062	GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS)	CVE-2022-39181	14/11/2022
ILVN-2022-0061	College Management System v1.0 - SQL Injection (SQLi)	CVE-2022-39180	14/11/2022
ILVN-2022-0060	College Management System v1.0 - Authenticated remote code execution	CVE-2022-39179	14/11/2022
ILVN-2022-0059	Webvendome - webvendome Internal Server IP Disclosure	CVE-2022-39178	13/11/2022
ILVN-2022-0058	webvendome - webvendome SQL Injection	CVE-2022-36787	13/11/2022
ILVN-2022-0057	DLINK - DSL-224 Post-auth PCE	CVE-2022-36786	07/11/2022
ILVN-2022-0056	D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass	CVE-2022-36785	07/11/2022
ILVN-2022-0055	Elsight – Elsight Halo Remote Code Execution (RCE)	CVE-2022-36784	27/10/2022
ILVN-2022-0054	AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS)	CVE-2022-36783	03/10/2022
ILVN-2022-0053	Pal Electronics Systems - Pal Gate Authorization Errors	CVE-2022-36782	07/09/2022
ILVN-2022-0052	WiseConnect - ScreenConnect Session Code Bypass	CVE-2022-36781	07/09/2022
ILVN-2022-0051	Avdor CIS - crystal quality Credentials Management Errors	CVE-2022-36780	01/09/2022
ILVN-2022-0050	PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection	CVE-2022-36779	21/08/2022
ILVN-2022-0049	Synel - eHarmony Stored XSS	CVE-2022-36778	21/08/2022
ILVN-2022-0048	Tabit - giftcard stealth	CVE-2022-34776	16/08/2022
ILVN-2022-0047	Tabit - Excessive data exposure	CVE-2022-34775	16/08/2022
ILVN-2022-0046	Tabit - Arbitrary account modification	CVE-2022-34774	16/08/2022
ILVN-2022-0045	Tabit - HTTP Method manipulation	CVE-2022-34773	16/08/2022
ILVN-2022-0044	Tabit - password enumeration	CVE-2022-34772	16/08/2022
ILVN-2022-0043	Tabit - arbitrary SMS send on Tabits behalf	CVE-2022-34771	16/08/2022
ILVN-2022-0042	Tabit - sensitive information disclosure	CVE-2022-34770	16/08/2022
ILVN-2022-0041	Michlol - rashim web interface Insecure direct object references (IDOR)	CVE-2022-34769	02/08/2022
ILVN-2022-0040	Supersmart.me - Walk Through Performing unauthorized actions on other customers	CVE-2022-34768	02/08/2022
ILVN-2022-0039	ALLNET Gmbh - ADSL/VDSL Router inkl. Modem and Wlan Authorization Bypass	CVE-2022-34767	19/07/2022
ILVN-2022-0038	Supersmart.me – Walk Through access to business information without authentication	CVE-2022-30628	18/07/2022
ILVN-2022-0035	Chcnav - P5E GNSS Directory listing	CVE-2022-30625	13/07/2022
ILVN-2022-0036	Chcnav - P5E GNSS API not secure	CVE-2022-30626	13/07/2022
ILVN-2022-0037	Chcnav - P5E GNSS Information disclosure hard coded credentials	CVE-2022-30627	13/07/2022
ILVN-2022-0034	Chcnav - P5E GNSS Authentication bypass admin password reset	CVE-2022-30624	13/07/2022
ILVN-2022-0033	Chcnav - P5E GNSS Authentication bypass	CVE-2022-30623	13/07/2022
ILVN-2022-0032	Chcnav - P5E GNSS Information disclosure	CVE-2022-30622	13/07/2022
ILVN-2022-0031	Cellinx NVT – IP PTZ Camera local file inclusion	CVE-2022-30621	06/07/2022
ILVN-2022-0030	Cellinx NVT – IP PTZ Camera Privilege Escalation	CVE-2022-30620	06/07/2022
ILVN-2022-0029	Agile Point - Agile Point NX SQL injection (SQLi)	CVE-2022-30619	27/06/2022
ILVN-2022-0028	Priority - Priority web Insecure direct object references (IDOR)	CVE-2022-23173	27/06/2022
ILVN-2022-0027	Priority - Priority User Enumeration	CVE-2022-23172	26/06/2022
ILVN-2022-0026	AtlasVPN - Privilege Escalation	CVE-2022-23171	20/06/2022

ILVN-2022-0025	SysAid - Okta SSO integration	CVE-2022-23170	13/06/2022
ILVN-2022-0024	Amodat – Mobile Application Gateway SQL Injection (SQLi)	CVE-2022-23169	09/06/2022
ILVN-2022-0023	Amodat – Mobile Application Gateway SQL Injection (SQLi)	CVE-2022-23168	09/06/2022
ILVN-2022-0022	Amodat – Mobile Application Gateway Local File Inclusion (LFI)	CVE-2022-23167	09/06/2022
ILVN-2022-0018	Sysaid – sysaid Open Redirect	CVE-2022-22797	09/05/2022
ILVN-2022-0021	Sysaid – Sysaid Local File Inclusion (LFI)	CVE-2022-23166	09/05/2022
ILVN-2022-0020	Sysaid – Sysaid 14.2.0 Reflected Cross-Site Scripting (XSS)	CVE-2022-23165	09/ 05/2022
ILVN-2022-0019	Sysaid – Pro Plus Edition, SysAid Help Desk Broken Access Control	CVE-2022-22798	09/05/2022
ILVN-2022-0017	Sysaid – sysaid Account Takeover	CVE-2022-22796	09/05/2022
ILVN-2022-0016	Signiant – Manager + Agents XML External Entity (XXE)	CVE-2022-22795	01/03/2022
ILVN-2022-0015	Cybonet - PineApp Mail Relay	CVE-2022-22794	15/02/2022
ILVN-2022-0014	Cybonet - PineApp Mail Relay	CVE-2022-22793	15/02/2022
ILVN-2022-0013	MobiSoft - MobiPlus	CVE-2022-22792	01/02/2022
ILVN-2022-0012	SYNEL - eharmony version 8.0.2.3	CVE-2022-22791	25/01/2022
ILVN-2022-0011	SYNEL - eharmony version 8.0.2.3	CVE-2022-22790	25/01/2022
ILVN-2022-0010	Charactell - FormStorm Enterprise	CVE-2022-22789	19/01/2022
ILVN-2021-0009	ForeScout - SecureConnector Local Service DoS	CVE-2021-36724	29/12/2021
ILVN-2021-0008	Emuse - eServices / eNvoice Exposure Of Private Personal Information	CVE-2021-36723	28/12/2021
ILVN-2021-0007	Emuse - eServices / eNvoice SQL injection	CVE-2021-36722	28/12/2021
ILVN-2021-0006	Sysaid - Sysaid API User Enumeration	CVE-2021-36721	13/12/2021
ILVN-2021-0005	Cybonet – PineApp Mail Secure	CVE-2021-36720	29/11/2021
ILVN-2021-0004	Cybonet – PineApp Mail Secure	CVE-2021-36719	29/11/2021
ILVN-2021-0003	Synel – Credentials Management Errors	CVE-2021-36718	15/11/2021
ILVN-2021-0002	Synerion TimeNet - Directory Traversal	CVE-2021-36717	01/09/2021
ILVN-2021-0001	CyberArk Identity - Username Enumeration	CVE-2021-37151	22/08/2021

GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS)

ILVN-ID: ILVN-2022-0062
CVE-ID: CVE-2022-39181
Affected Products: GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS)
Description: GLPI - Reports plugin for GLPI Reflected Cross-Site-Scripting (RXSS).
Type 1: Reflected XSS (or Non-Persistent) - The server reads data directly from the HTTP request and reflects it back in the HTTP response. Reflected XSS exploits occur when an attacker causes a victim to supply dangerous content to a vulnerable web application, which is then reflected back to the victim and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to the victim. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces a victim to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the victim, the content is executed by the victim's browser.
Credit/Acknowledgments: Moriel Harush, Dudu Moyal - EY – Hacktics.
Public Date: 14/11/22

College Management System v1.0 - SQL Injection (SQLi)

ILVN-ID: ILVN-2022-0061
CVE-ID: CVE-2022-39180
Affected Products: College Management System v1.0 - SQL Injection (SQLi)
Description: College Management System v1.0 - SQL Injection (SQLi).
By inserting SQL commands to the username and password fields in the login.php page
Credit/Acknowledgments: Liav Gutman
Public Date: 14/11/22

College Management System v1.0 - Authenticated remote code execution

ILVN-ID: ILVN-2022-0060

CVE-ID: CVE-2022-39179
Affected Products: College Management System v1.0 - Authenticated remote code execution
Description: College Management System v1.0 - Authenticated remote code execution.
An admin user (the authentication can be bypassed using SQL Injection that mentioned in my other report) can upload .php file that contains malicious code via student.php file.
Credit/Acknowledgments: Liav Gutman
Public Date: 14/11/22

Webvendome - webvendome Internal Server IP Disclosure

ILVN-ID: ILVN-2022-0059
CVE-ID: CVE-2022-39178
Affected Products: Webvendome - webvendome Internal Server IP Disclosure.
Description: Webvendome - webvendome Internal Server IP Disclosure.
Send GET Request to the request which is shown in the picture.
Internal Server IP and Full path disclosure.
Solution: Update to the latest version.
Credit/Acknowledgments: Dudu Moyal , Moriel Harush , Gad Abuhatziera - Sophtix Security LTD.
Public Date: 13/11/22

webvendome - webvendome SQL Injection

ILVN-ID: ILVN-2022-0058
CVE-ID: CVE-2022-36787
Affected Products: webvendome - webvendome SQL Injection.
Description: webvendome - webvendome SQL Injection.
SQL Injection in the Parameter " DocNumber"
Request :
Get Request :
/webvendome/showfiles.aspx?jobnumber=nullDoc Number=HERE.
Solution: Update to the latest version.
Credit/Acknowledgments: Dudu Moyal , Moriel Harush , Gad Abuhatziera - Sophtix Security LTD.
Public Date: 13/11/22

CVE Advisories

Open All Close All

D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass

ILVN-ID: ILVN-2022-0056
CVE-ID: CVE-2022-36785
Affected Products: D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass.
Description: D-Link – G integrated Access Device4 Information Disclosure & Authorization Bypass.
*Information Disclosure –
file contains a URL with private IP at line 15 "login.asp" A. The
window.location.href =http://192.168.1.1/setupWizard.asp"
"admin" – contains default username value "login.asp" B. While accessing the web interface, the login form at

*Authorization Bypass –
URL by "setupWizard.asp' while it blocks direct access to – the web interface does not properly validate user identity variables values located at the client side, it is available to access it without a "login_glag" and "login_status" checking browser and to read the admin user credentials for the web interface.
Credit/Acknowledgments: MetaData
Public Date: 07/11/22

DLINK - DSL-224 Post-auth PCE

ILVN-ID: ILVN-2022-0057
CVE-ID: CVE-2022-36786
Affected Products: DLINK - DSL-224 Post-auth PCE.

Description: DLINK - DSL-224 Post-auth PCE.
DLINK router has an interface where you can configure NTP servers (Network Time Protocol) via jsonrpc API.
It is possible to inject a command through this interface that will run with ROOT permissions on the router.
Credit/Acknowledgments: Nerya Zadkani
Public Date: 07/11/22

Elsight – Elsight Halo Remote Code Execution (RCE)

ILVN-ID: ILVN-2022-0055
CVE-ID: CVE-2022-36784
Affected Products: Elsight – Elsight Halo Remote Code Execution (RCE)
Description: Elsight – Elsight Halo Remote Code Execution (RCE)
Elsight Halo web panel allows us to perform connection validation.
through the POST request :
/api/v1/nics/wifi/wlan0/ping
we can abuse DESTINATION parameter and leverage it to remote code execution.
Solution: Update to version 10.6.1
Credit/Acknowledgments: Dudu Moyal ,Moriel Harush
Public Date: 27/10/22

AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS)

ILVN-ID: ILVN-2022-0054
CVE-ID: CVE-2022-36783
Affected Products: AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS)
Description: AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS)
A malicious user injects JavaScript code into a parameter called IntersectudRule on the search/result.html page. The malicious user changes the request from POST to GET and sends the URL to another user (victim).
JavaScript code is executed on the browser of the other user.
Solution: Update released for the following versions:
For A32.0 : A32.0.580-277
For A32.10 : A32.10.410-212
For A32.20 : A32.20.230-35
Credit/Acknowledgments: Dean Aviani - Hacktics EY
Public Date: 03/10/22

Pal Electronics Systems - Pal Gate Authorization Errors

ILVN-ID: ILVN-2022-0053
CVE-ID: CVE-2022-36782
Affected Products: Pal Electronics Systems - Pal Gate Authorization Errors.
Description: Pal Electronics Systems - Pal Gate Authorization Errors.
The vulnerability is an authorization problem in PalGate device management android client app.
Gates of bulidings and parking lots with a simple button in any smartphone.
The API was found after a decompiling and static research using Jadx, and a dynamic analasys using Frida.
The attacker can iterate over all the IOT devices to see every entry and exit, on every gate and device all over the world,
he can also scrape the server and create a user's DB with full names and phone number of over 2.8 million users, and to see all of the users' movement in and out of gates, even in real time.
Solution: Update to the latest version.
Credit/Acknowledgments: Tal Saadi
Public Date: 07/09/22

WiseConnect - ScreenConnect Session Code Bypass

ILVN-ID: ILVN-2022-0052
CVE-ID: CVE-2022-36781
Affected Products: WiseConnect - ScreenConnect Session Code Bypass.

Description: WiseConnect - ScreenConnect Session Code Bypass.
An attacker would have to use a proxy to monitor the traffic, and perform a brute force on the session code in order to get in.
Sensitive data about the company , get in a session.
Solution: Update to version 22.7.
Credit/Acknowledgments: Gad Abuhatziera – Sophtix Security LTD
Public Date: 07/09/22

Avdor CIS - crystal quality Credentials Management Errors

ILVN-ID: ILVN-2022-0051
CVE-ID: CVE-2022-36780
Affected Products: Avdor CIS - crystal quality Credentials Management Errors
Description: Avdor CIS - crystal quality Credentials Management Errors.
The product is phone call recorder, you can hear all the recorded calls without authenticate to the system.
Attacker sends crafted URL to the system :
ip:port//V=2;ChannelID=number;Ext=number;Command=startLM;Client=number;Request=number;R=number
number - id of the recorded number.
Solution: Update to the latest version.
Credit/Acknowledgments: Dudu Moyal – EY Hacktics.
Public Date: 01/09/22

PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection

ILVN-ID: ILVN-2022-0050
CVE-ID: CVE-2022-36779
Affected Products: PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection
Description: PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection

- Proscend M330-w / M33-W5 / M350-5G / M350-W5G / M350-6 / M350-W6 / M301-G / M301-GW
- ADVICE ICR 111WG /

https://www.proscend.com/en/category/industrial-Cellular-Router/industrial-Cellular-Router.html
https://cdn.shopify.com/s/files/1/0036/9413/3297/files/ADVICE_Industrial_4G_LTE_Cellular_Router_ICR111WG.pdf?v=1620814301
Solution: Update released for the following versions:

- Proscend M330-w / M330-W5 Plan to fix on V1.11
- Proscend M350-5G / M350-W5G / M350-6 / M350-W6 Fixed on V1.02
- Proscend M301-G / M301-GW Fixed on V2.20
- ADVICE ICR 111WG / Plan to fix on V1.11

Credit/Acknowledgments: MetaData
Public Date: 21/08/22

Synel - eHarmony Stored XSS

ILVN-ID: ILVN-2022-0049
CVE-ID: CVE-2022-36778
Affected Products: Synel - eHarmony Stored XSS
Description: Synel - eHarmony Stored XSS
insert HTML / js code inside input
how to get to the vulnerable input :
Workers > worker nickname > inject in this input the code.
Solution: Update to eHarmony v11.
Credit/Acknowledgments: Moriel Harush - Sophtix Security LTD
Public Date: 21/08/22

Tabit - giftcard stealth

ILVN-ID: ILVN-2022-0048
CVE-ID: CVE-2022-34776
Affected Products: Tabit - giftcard stealth.
Description: Tabit - giftcard stealth.
Several APIs on the web system display, without authorization, sensitive information such as health statements, previous bills in a specific restaurant, alcohol consumption and smoking habits.
Each of the described APIs, has in its URL one or more MongoDB ID which is not so simple to enumerate. However, they each receive a 'tiny URL' in tabits domain, in the form of https://tbit.be/{suffix} with suffix being a 5 character long string containing numbers, lower and upper case letters. It is not so simple to enumerate them all, but really easy to find some that work and lead to a personal endpoint.
Furthermore, the redirect URL disclosed the MongoDB IDs discussed above, and we could use them to query other endpoints disclosing more personal information.
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - Excessive data exposure

ILVN-ID: ILVN-2022-0047
CVE-ID: CVE-2022-34775
Affected Products: Tabit - Excessive data exposure.
Description: Tabit - Excessive data exposure.
Another endpoint mapped by the tiny url, was one for reservation cancellation, containing the MongoDB ID of the reservation, and organization. This can be used to query the http://tgm-api.tabit.cloud/rsv/management/{reservationId}?organization={orgId} API which returns a lot of data regarding the reservation (OWASP: API3):
Name, mail, phone number, the number of visits of the user to this specific restaurant, the money he spent there, the money he spent on alcohol, whether he left a deposit etc.
This information can easily be used for a phishing attack.
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - Arbitrary account modification

ILVN-ID: ILVN-2022-0046
CVE-ID: CVE-2022-34774
Affected Products: Tabit - Arbitrary account modification.
Description: Tabit - Arbitrary account modification.
One of the endpoints mapped by the tiny URL, was a page where an adversary can modify personal details, such as email addresses and phone numbers of a specific user in a restaurant's loyalty program. Possibly allowing account takeover (the mail can be used to reset password).
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - HTTP Method manipulation

ILVN-ID: ILVN-2022-0045
CVE-ID: CVE-2022-34773
Affected Products: Tabit - HTTP Method manipulation.
Description: Tabit - HTTP Method manipulation.
https://bridge.tabit.cloud/configuration/addresses-query - can be POST-ed to add addresses to the DB.
This is an example of OWASP:API8 – Injection.
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - password enumeration

ILVN-ID: ILVN-2022-0044
CVE-ID: CVE-2022-34772
Affected Products: Tabit - password enumeration.
Description: Tabit - password enumeration.
The passwords for the Tabit system is a 4 digit OTP. One can resend OTP and try logging in indefinitely. Once again, this is an example of OWASP: API4 - Rate limiting
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - arbitrary SMS send on Tabits behalf

ILVN-ID: ILVN-2022-0043
CVE-ID: CVE-2022-34771
Affected Products: Tabit - arbitrary SMS send on Tabits behalf.
Description: Tabit - arbitrary SMS send on Tabits behalf.
The resend OTP API of tabit allows an adversary to send messages on tabits behalf to anyone registered on the system - the API receives the parameters: phone number, and CustomMessage, We can use that API to craft malicious messages to any user of the system. In addition, the API probably has some kind of template injection potential. When entering {{OTP}} in the custom message field it is formatted into an OTP.
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Tabit - sensitive information disclosure

ILVN-ID: ILVN-2022-0042
CVE-ID: CVE-2022-34770
Affected Products: Tabit - sensitive information disclosure.
Description: Tabit - sensitive information disclosure.
Several APIs on the web system display, without authorization, sensitive information such as health statements, previous bills in a specific restaurant, alcohol consumption and smoking habits.
Each of the described API's, has in its URL one or more MongoDB ID which is not so simple to enumerate.
However, they each receive a 'tiny URL' in Tabit's domain, in the form of https://tbit.be/{suffix} with suffix being a 5 characters long string containing numbers, lower- and upper-case letters.
It is not so simple to enumerate them all, but really easy to find some that work and lead to a personal endpoint.
This is both an example of OWASP: API4 - rate limiting and OWASP: API1 - Broken object level authorization.
Furthermore, the redirect URL disclosed the MongoDB IDs discussed above, and we could use them to query other endpoints disclosing more personal information.
For example:
The URL https://tabitisrael.co.il/online-reservations/health-statement?orgId={org_id}&healthStatementId={health_statement_id} is used to invite friends to fill a health statement before attending the restaurant. We can use the health_statement_id to access the https://tgm-api.tabit.cloud/health-statement/{health_statement_id} API which disclose medical information as well as id number.
Solution: Update to version 3.27.0.
Credit/Acknowledgments: Guy Ben Simhon - Noname Security
Public Date: 16/08/22

Michlol - rashim web interface Insecure direct object references (IDOR)

ILVN-ID: ILVN-2022-0041
CVE-ID: CVE-2022-34769
Affected Products: Michlol - rashim web interface Insecure direct object references (IDOR).
Description: Michlol - rashim web interface Insecure direct object references (IDOR).
First of all, the attacker needs to login.
After he performs log into the system there are some functionalities that the specific user is not allowed to perform.
However all the attacker needs to do in order to achieve his goals is to change the value of the ptMsl parameter and then the attacker can access sensitive data that he not supposed to access because its belong to another user.
Solution: Update to version 187.4392.
Credit/Acknowledgments: Gad Abuhatzera
Public Date: 02/08/22

Supersmart.me - Walk Through Performing unauthorized actions on other customers

ILVN-ID: ILVN-2022-0040
CVE-ID: CVE-2022-34768
Affected Products: Supersmart.me - Walk Through Performing unauthorized actions on other customers.
Description: Supersmart.me - Walk Through Performing unauthorized actions on other customers.
Supersmart.me has a product designed to conduct smart shopping in stores.
The customer receives a coder (or using an Android application) to scan at the beginning of the purchase the QR CODE on the cart, and then all the products he wants to purchase.
At the end of the purchase the customer can pay independently.
During the research it was discovered that it is possible to reset another customer's cart without verification.
Because the number of purchases is serial.
Solution: Update to the latest version.
Credit/Acknowledgments: Nerya Zadkani
Public Date: 02/08/22

ALLNET Gmbh - ADSL/VDSL Router inkl. Modem and Wlan Authorization Bypass

ILVN-ID: ILVN-2022-0039
CVE-ID: CVE-2022-34767
Affected Products ALLNET Gmbh - ADSL/VDSL Router inkl. Modem and Wlan Authorization Bypass.
Description: ALLNET Gmbh - ADSL/VDSL Router inkl. Modem and Wlan Authorization Bypass.
Web page which "wizardpwd.asp" ALLNET Router model WR0500AC is prone to Authorization bypass vulnerability – the password, located at "admin" allows changing the http[s]://wizardpwd.asp/cgi-bin.
Does not validate the user's identity and can be accessed publicly.
Solution: Update to the latest version.
Credit/Acknowledgments: MetaData
Public Date: 19/07/2022

Supersmart.me – Walk Through access to business information without authentication

ILVN-ID: ILVN-2022-0038
CVE-ID: CVE-2022-30628
Affected Products Supersmart.me – Walk Through access to business information without authentication.
Description: Supersmart.me – Walk Through access to business information without authentication,
It was possible to download all receipts without authentication.
Must first access the API https://XXXX.supersmart.me/services/v4/customer/signin to get a TOKEN.
Then you can then access the API that provides invoice images based on the URL
https://XXXX.supersmart.me/services/v4/invoiceImg?orderId=XXXXX
Solution: Update to the latest version.
Credit/Acknowledgments: Nerya Zadkani
Public Date: 18/07/2022

Chcnav - P5E GNSS Directory listing

ILVN-ID: ILVN-2022-0035
CVE-ID: CVE-2022-30625
Affected Products Chcnav - P5E GNSS Directory listing.
Description: Chcnav - P5E GNSS Directory listing
Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences vary depending on which files are listed and accessible.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Chcnav - P5E GNSS API not secure

ILVN-ID: ILVN-2022-0036
CVE-ID: CVE-2022-30626
Affected Products Chcnav - P5E GNSS API not secure.
Description: Chcnav - P5E GNSS API not secure.
Browsing the path: http://ip/wifi_ap_pata_get.cmd, will show in the name of the existing access point on the component, and a password in clear text.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Chcnav - P5E GNSS Information disclosure hard coded credentials

ILVN-ID: ILVN-2022-0037
CVE-ID: CVE-2022-30627
Affected Products Chcnav - P5E GNSS Information disclosure hard coded credentials.
Description: Chcnav - P5E GNSS Information disclosure hard coded credentials.
This vulnerability affects all of the company's products that also include the FW versions: update_i90_cv2.021_b20210104, update_i50_v1.0.55_b20200509, update_x6_v2.1.2_b202001127, update_b5_v2.0.9_b20200706. This vulnerability makes it possible to extract from the FW the existing user passwords on their operating systems and passwords.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Chcnav - P5E GNSS Authentication bypass admin password reset

ILVN-ID: ILVN-2022-0034
CVE-ID: CVE-2022-30624
Affected Products Chcnav - P5E GNSS Authentication bypass admin password reset.
Description: Chcnav - P5E GNSS Authentication bypass admin password reset.
Browsing the admin.html page allows the user to reset the admin password.
Also appears in the JS code for the password.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Chcnav - P5E GNSS Authentication bypass

ILVN-ID: ILVN-2022-0033
CVE-ID: CVE-2022-30623
Affected Products Chcnav - P5E GNSS Authentication bypass.
Description: Chcnav - P5E GNSS Authentication bypass.
The server checks the user's cookie in a non-standard way, and a value is entered in the cookie value name of the status and its value is set to true to bypass the identification with the system using a username and password.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Chcnav - P5E GNSS Information disclosure

ILVN-ID: ILVN-2022-0032
CVE-ID: CVE-2022-30622
Affected Products Chcnav - P5E GNSS Information disclosure.
Description: Chcnav - P5E GNSS Information disclosure.
Disclosure of information - the system allows you to view usernames and passwords without permissions, thus it will be possible to enter the system. Path access: http://api/sys_username_passwd.cmd - The server loads the request clearly by default.
Disclosure of hard-coded credit information within the JS code sent to the customer within the Login.js file is a strong user (which is not documented) and also the password, which allow for super-user access.
Username: chcadmin, Password: chcpassword.
Credit/Acknowledgments: MetaData
Public Date: 13/07/2022

Cellinx NVT – IP PTZ Camera Privilege Escalation

ILVN-ID: ILVN-2022-0030
CVE-ID: CVE-2022-30620
Affected Products Cellinx NVT – IP PTZ Camera Privilege Escalation.
Description: Cellinx NVT – IP PTZ Camera Privilege Escalation.
On Cellinx Camera with guest enabled, attacker with web access can elevate privileges to administrative: "1" to "0" privileges by changing the following cookie values from "is_admin", "showConfig".
Administrative Privileges which allows changing various configuration in the camera.
Credit/Acknowledgments: MetaData
Public Date: 06/07/2022

Cellinx NVT – IP PTZ Camera local file inclusion

ILVN-ID: ILVN-2022-0031
CVE-ID: CVE-2022-30621
Affected Products Cellinx NVT – IP PTZ Camera local file inclusion.
Description: Cellinx NVT – IP PTZ Camera local file inclusion.
Allows a remote user to read files on the camera's OS "GetFileContent.cgi".
Reading arbitrary files on the camera's OS as root user.
Credit/Acknowledgments: MetaData
Public Date: 06/07/2022

CVE Advisories

Open All Close All

Agile Point - Agile Point NX SQL injection (SQLi)

ILVN-ID: ILVN-2022-0029
CVE-ID: CVE-2022-30619
Affected Products Agile Point - Agile Point NX SQL injection (SQLi).
Description: Agile Point - Agile Point NX SQL injection (SQLi).
Editable SQL Queries behind Base64 encoding sending from the Client-Side to The Server-Side for a particular API used in legacy Work Center module.
He attack is available for any authenticated user, in any kind of rule.
under the function :
/AgilePointServer/Extension/FetchUsingEncodedData
in the parameter:
EncodedData
Solution: Update to version V8.0.
Credit/Acknowledgments: Osher Assor.
Public Date: 27/06/2022

Priority - Priority web Insecure direct object references (IDOR)

ILVN-ID: ILVN-2022-0028
CVE-ID: CVE-2022-23173
Affected Products: Priority - Priority web Insecure direct object references (IDOR).
Description: Priority - Priority web Insecure direct object references (IDOR).
this vulnerability affect user that even not allowed to access via the web interface.
First of all, the attacker needs to access the "Login menu - demo site" then he can see in this menu all the functionality of the application. If the attacker will try to click on one of the links, he will get an answer that he is not authorized because he needs to log in with credentials.
after he performed log in to the system there are some functionalities that the specific user is not allowed to perform because he was configured with low privileges however all the attacker need to do in order to achieve his goals is to change the value of the prog step parameter from 0 to 1 or more and then the attacker could access to some of the functionality the web application that he couldn't perform it before the parameter changed.
Solution: Update to version V22.0.
Credit/Acknowledgments: Gad Abuhatzeira - Sophtix Security LTD.
Public Date: 27/06/2022

Priority - Priority User Enumeration

ILVN-ID: ILVN-2022-0027
CVE-ID: CVE-2022-23172
Affected Products: Priority - Priority User Enumeration
Description: Priority - Priority User Enumeration.
An attacker can access to "Forgot my password" button, as soon as he puts users is valid in the system, the system would issue a message that a password reset email had been sent to user.
This way you can verify which users are in the system and which are not.
Solution: Update to version V22.0.
Credit/Acknowledgments: Dudu Moyal - Sophtix Security LTD.
Public Date: 26/06/2022

AtlasVPN - Privilege Escalation

ILVN-ID: ILVN-2022-0026
CVE-ID: CVE-2022-23171

Affected Products: AtlasVPN - Privilege Escalation
Description: AtlasVPN - Privilege Escalation
Lack of proper security controls on named pipe messages can allow an attacker with low privileges to send a malicious payload and gain SYSTEM permissions on a windows computer where the AtlasVPN client is installed.
Solution: Update version 2.4.2 of the Windows app.
Credit/Acknowledgments: Alex Katziv
Public Date: 20/06/2022

SysAid - Okta SSO integration

ILVN-ID: ILVN-2022-0025
CVE-ID: CVE-2022-23170

Affected Products: SysAid - Okta SSO integration
Description: SysAid - Okta SSO integration - was found vulnerable to XML External Entity Injection vulnerability. Any SysAid environment that uses the Okta SSO integration might be vulnerable.
An unauthenticated attacker could exploit the XXE vulnerability by sending a malformed POST request to the identity provider endpoint. An attacker can extract the identity provider endpoint by decoding the SAMLRequest parameter's value and searching for the AssertionConsumerServiceURL parameter's value.
It often allows an attacker to view files on the application server filesystem and interact with any back-end or external systems that the application can access.
In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.
Solution: Update to 22.1.50 cloud version, or to 22.1.64 on premise version.
Credit/Acknowledgments: Niv Levy - CyberArk
Public Date: 13/06/2022

Amodat – Mobile Application Gateway SQL Injection Error Based (SQLi)

ILVN-ID: ILVN-2022-0024

CVE-2022-23169

Affected Products: Amodat - Mobile Application Gateway SQL Injection Error Based

Description: Amodat – Mobile Application Gateway SQL Injection Error Based - full control on SQL.
attacker needs to craft a SQL payload.
the vulnerable parameter is "agentid"
must be authenticated to the admin panel.

Solution: Update to 7.12.00.09 version.

Credit/Acknowledgments: Moriel Harush Dudu Moyal Gad Abuhatziera

Public Date: 09/06/2022

Amodat – Mobile Application Gateway SQLi Injection (SQLi)

ILVN-ID: ILVN-2022-0023

CVE-2022-23168

Affected Products: Amodat - Mobile Application Gateway SQL Injection (SQLi)

Description: Amodat – Mobile Application Gateway SQL Injection (SQLi) - Access to the internal system and system management.
The attacker could get access to the database.
The sql injection is in the username parameter at the login panel:
username : admin'--

Solution: Update to 7.12.00.09 version.

Credit/Acknowledgments: Moriel Harush Dudu Moyal Gad Abuhatziera

Public Date: 09/06/2022

Amodat – Mobile Application Gateway Local File Inclusion (LFI)

ILVN-ID: ILVN-2022-0022

CVE-2022-23167

Affected Products: Amodat - Mobile Application Gateway Local File Inclusion (LFI)

Description: Amodat – Mobile Application Gateway Local File Inclusion (LFI) - Reading sensitive files in the system.
Attacker crafts a GET request to: /mobile/downloadfile.aspx? Filename =../.. /windows/boot.ini
the LFI is UNAUTHENTICATED and Reading sensitive files in the system

Solution: Update to 7.12.00.09 version.

Credit/Acknowledgments: Moriel Harush Dudu Moyal Gad Abuhatziera

Public Date: 09/06/2022

Sysaid – sysaid Open Redirect

ILVN-ID: ILVN-2022-0018
CVE-ID: CVE-2022-22797

Affected Products: Sysaid – sysaid Open Redirect
Description: Sysaid – sysaid Open Redirect - An Attacker can change the redirect link at the parameter "redirectURL" from"GET" request from the url location: /CommunitySSORedirect.jsp?redirectURL=https://google.com.
Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.
Solution: Update to 22.1.50 cloud version, or to 22.1.64 on premise version.
Credit/Acknowledgments: Moriel Harush - Sophtix Security LTD
Public Date: 09/05/2022

Sysaid – Sysaid Local File Inclusion (LFI)

ILVN-ID: ILVN-2022-0021
CVE-ID: CVE-2022-23166

Affected Products: Sysaid – Sysaid Local File Inclusion (LFI)

Description: Sysaid – Sysaid Local File Inclusion (LFI) – An unauthenticated attacker can access to the system by accessing to "/lib/tinymce/examples/index.html" path. in the "Insert/Edit Embedded Media" window Choose Type : iFrame and File/URL : [here is the LFI]
Solution: Update to 22.2.20 cloud version, or to 22.1.64 on premise version.

Credit/Acknowledgments: Dudu Moyal - Sophtix Security LTD
Public Date: 09/05/2022

Sysaid – Sysaid 14.2.0 Reflected Cross-Site Scripting (XSS)

ILVN-ID: ILVN-2022-0020
CVE-ID: CVE-2022-23165

Affected Products: Sysaid – Sysaid 14.2.0 Reflected Cross-Site Scripting (XSS).
Description: Sysaid – Sysaid 14.2.0 Reflected Cross-Site Scripting (XSS) - The parameter "helpPageName" used by the page "/help/treecontent.jsp" suffers from a Reflected Cross-Site Scripting vulnerability.
For an attacker to exploit this Cross-Site Scripting vulnerability, it's necessary for the affected product to expose the Offline Help Pages.
An attacker may gain access to sensitive information or execute client-side code in the browser session of the victim user.
Furthermore, an attacker would require the victim to open a malicious link.
An attacker may exploit this vulnerability in order to perform phishing attacks. The attacker can receive sensitive data like server details, usernames, workstations, etc.
He can also perform actions such as uploading files, deleting calls from the system.
Solution: Update to 22.2.20 cloud version, or to 22.1.64 on premise version.
Credit/Acknowledgments: Robert Catalin Raducioiu,, Francesco Di Castri
Public Date: 09/05/2022

Sysaid – Pro Plus Edition, SysAid Help Desk Broken Access Control

ILVN-ID: ILVN-2022-0019
CVE-ID: CVE-2022-22798

Affected Products: Sysaid – Pro Plus Edition, SysAid Help Desk Broken Access Control
Description: Sysaid – Pro Plus Edition, SysAid Help Desk Broken Access Control v20.4.74 b10, v22.1.20 b62, v22.1.30 b49 - An attacker needs to log in as a guest after that the system redirects him to the service portal or EndUserPortal.JSP, then he needs to change the path in the URL to /ConcurrentLogin%2ejsp after that he will receive an error message with a login button, by clicking on it, he will connect to the system dashboard.
The attacker can receive sensitive data like server details, usernames, workstations, etc.
He can also perform actions such as uploading files, deleting calls from the system.
Solution: Update to 22.1.50 cloud version, or to 22.1.64 on premise version.
Credit/Acknowledgments: Gad Abuhatzeira, Alon Zuker- Sophtix Security LTD
Public Date: 09/05/2022

Sysaid – sysaid system Account Takeover

ILVN-ID: ILVN-2022-0017
CVE-ID: CVE-2022-22796

Affected Products: Sysaid – sysaid system Account Takeover
Description: Sysaid – sysaid system Account Takeover - An attacker can bypass the authentication process by accessing to: /wmiwizard.jsp, Then to: /ConcurrentLogin.jsp, then click on the login button, and it will redirect you to /home.jsp without any authentication.
Solution: Update to 21.1.30 cloud version, or to 21.4.45 on premise version.
Credit/Acknowledgments: Dudu Moyal, Gad Abuhatziera, Moriel Harush, Alon Zuker - Sophtix Security LTD
Public Date: 09/05/2022

Signiant – Manager + Agents XML External Entity (XXE)

ILVN-ID: ILVN-2022-0016
CVE-ID: CVE-2022-22795

Affected Products: Signiant – Manager + Agents

Description: Signiant – Manager + Agents XML External Entity (XXE) - Extract internal files of the affected machine.
The product is running with root on Linux systems and NT/Authority on windows systems, which allows an attacker to access and extract any file on the systems, such as passwd, shadow, hosts and so on.

By gaining access to these files, attackers can steal sensitive information from the victims machine.

Solution: All of 13.5, 14.1, and 15.1 have an update available. The mitigation involved adding a filter that validates for external dtd.

Credit/Acknowledgments: Anton Golotin

Public Date: 01/03/2022

Cybonet - PineApp Mail Relay Unauthenticated SQL Injection

ILVN-ID: ILVN-2022-0015

CVE-ID: CVE-2022-22794

Affected Products: Cybonet - PineApp Mail Relay

Description: Cybonet - PineApp Mail Relay Unauthenticated SQL Injection to Remote Code Execution. Attacker can send a request to:

/manage/emailrichment/userlist.php?CUSTOMER_ID_INNER=1

/admin/emailrichment/userlist.php?CUSTOMER_ID_INNER=1

/manage/emailrichment/usersunlist.php?CUSTOMER_ID_INNER=1

/admin/emailrichment/usersunlist.php?CUSTOMER_ID_INNER=1

and by doing that, the attacker can run Remote Code Execution in one liner.

Solution: A patch was released with a hardening of the input validation.

Credit/Acknowledgments: Dudu Moyal - Sophtix Security LTD , Gad Abuhatzeira - Sophtix Security LTD

Public Date: 15/02/2021

Cybonet - PineApp Mail Relay Local File Inclusion

ILVN-ID: ILVN-2022-0014

CVE-ID: CVE-2022-22793

Affected Products: Cybonet - PineApp Mail Relay

Description: Cybonet - PineApp Mail Relay Local File Inclusion. Attacker can send a request to :

/manage/mailpolicymtm/log/eml_viewer/email.content.body.php?filesystem_path=ENCDODED PATH

and by doing that, the attacker can read Local Files inside the server.

Solution: A patch was released with code hardening by limiting the file path

Credit/Acknowledgments: Dudu Moyal - Sophtix Security LTD

Public Date: 15/02/2021

MobiSoft - MobiPlus User Take Over and Improper Handling of URL Parameters

ILVN-ID: ILVN-2022-0013

CVE-ID: CVE-2022-22792

Affected Products: MobiSoft - MobiPlus

Description: MobiSoft - MobiPlus User Take Over and Improper Handling of url Parameters. Attacker can navigate to specific url which will expose all the users and password in clear text. http://IP/MobiPlusWeb/Handlers/MainHandler.ashx?MethodName=GridData&GridName=Users

Solution: An update was released which addresses the issue

Credit/Acknowledgments: Dudu Moyal - Sophtix Security LTD

Public Date: 01/02/2021

SYNEL - eharmony Authenticated Blind & Stored XSS

ILVN-ID: ILVN-2022-0012
CVE-ID: CVE-2022-22791

Affected Products: SYNEL - eharmony version 8.0.2.3

Description: SYNEL - eharmony Authenticated Blind & Stored XSS.
SYNEL - eharmony Authenticated Blind & Stored XSS. Inject JS code into the \"comments\" field could lead to potential stealing of cookies, loading of HTML tags and JS code onto the system. Solution: A patch was released, Update to eharmony version 11

Solution: A patch was released, Update to eharmony version 11

Credit/Acknowledgments: Moriel Harush - Sophtix Security LTD

Public Date: 25/01/2021

SYNEL - eharmony Directory Traversal

ILVN-ID: ILVN-2022-0011

CVE-ID: CVE-2022-22790

Affected Products: SYNEL - eharmony version 8.0.2.3

Description: SYNEL - eharmony Directory Traversal.
Directory Traversal - is an attack against a server or a Web application aimed at unauthorized access to the file system.\non the \"Name\" parameter the attacker can return to the root directory and open the host file. The path exposes sensitive files that users upload.

Solution: : A patch was released, Update to eharmony version 11

Credit/Acknowledgments: Dudu Moyal & Gad Abuhatziera - Sophtix Security LTD

Public Date: 25/01/2022

Charactell - FormStorm Enterprise Account Take Over

ILVN-ID: ILVN-2022-0010

CVE-ID: CVE-2022-22789

Affected Products: Charactell - FormStorm Enterprise version 9.00.065

Description: Charactell - FormStorm Enterprise Account takeover – An attacker can modify (add, remove and update) passwords file for all the users. The xx_users.ini file in the FormStorm folder contains usernames in cleartext and an obfuscated password. Malicious user can take over an account by replacing existing password in the file.

Solution: A patch was released, Charactell - FormStorm Enterprise version 9.00.066

Credit/Acknowledgments: Michael Starchenko

Public Date: 19/01/2021

ForeScout - SecureConnector Local Service DoS

ILVN-ID: ILVN-2021-0009

CVE-ID: CVE-2021-36724

Affected Products: ForeScout - SecureConnector

Description: ForeScout - SecureConnector Local Service DoS - A low privileged user which doesn't have permissions to shut down the secure connector service writes a large amount of characters in the installationPath. This will cause the buffer to overflow and override the stack cookie causing the service to crash.

Solution: A HotFix was released

Credit/Acknowledgments: Alex Katziv - Novartis

Public Date: 28/12/2021

Emuse - eServices / eNvoice SQL injection

ILVN-ID: ILVN-2021-0007

CVE-ID: CVE-2021-36722

Affected Products: Emuse - eServices / eNvoice

Description: Emuse - eServices / eNvoice SQL injection can be used in various ways ranging from bypassing login authentication or dumping the whole database to full RCE on the affected endpoints.\nThe SQLi caused by CWE-209: Generation of Error Message Containig Sensetive Information, showing parts of the aspx code and the webroot location , information an attacker can leverage to further compromise the host.

Solution: The SQL injection vulnerability was fixed by Escaping All User-Supplied Input

Credit/Acknowledgments: Simon Kenin - ClearSky Cyber Security Ltd

Public Date: 28/12/2021

Emuse - eServices / eNvoice Exposure Of Private Personal Information

ILVN-ID: ILVN-2021-0008

CVE-ID: CVE-2021-36723

Affected Products: Emuse - eServices / eNvoice

Description: Emuse - eServices / eNvoice Exposure Of Private Personal Information due to lack of identification mechanisms and predictable IDs an attacker can scrape all the files on the service.

Solution: The Exposure Of Private Personal Information due to lack of identification mechanisms and predictable IDs vulnerability was fixed by adding security mechanisms and randomizing the IDs

Credit/Acknowledgments: Simon Kenin - ClearSky Cyber Security Ltd

Public Date: 28/12/2021

Sysaid - Sysaid API User Enumeration

ILVN-ID: ILVN-2021-0006

CVE-ID:CVE-2021-36721

Affected Products: Sysaid – version 20.4.74

Description: User Enumeration - Attacker sending requests to specific api path without any authorization could get users names from the LDAP.

Solution: Update to version 21.3.60

Credit/Acknowledgments: Dudu Moyal , Sophtix

Public Date: 13/12/2021

Cybonet - PineApp Mail Secure Reflected XSS

ILVN-ID: ILVN-2021-0005

CVE-ID: CVE-2021-36720

Affected Products: Cybonet - PineApp Mail Secure

Description: Reflected XSS - Attacker sending a request to :/blocking.php?url=<script>alert(1)</script> potentially stealing cookies .

Solution: Update to version 5.2.1 - Code hardening by adding an extra layer of input validations

Credit/Acknowledgments: Moriel Harush , Sophtix

Public Date: 29/11/2021

Cybonet - PineApp Mail Secure Authenticated Remote Code Execution

ILVN-ID: ILVN-2021-0004

CVE-ID: CVE-2021-36719

Affected Products: Cybonet - PineApp Mail Secure

Description: Attacker can upload php reverse shell , When sending a POST to "/manage/main_incs_nicUpload.php" path. The attacker must be logged in as a user to the Pineapp system.
The attacker exploits the vulnerable nicUpload.php file to upload a malicious file, Thus taking over the server and running remote code.

Solution: Update to version 5.2.1 - Code hardening by limiting the upload file to only limited images file types

Credit/Acknowledgments: Dudu Moyal , Sophtix

Public Date: 29/11/2021

Synel – Credentials Management Errors

ILVN-ID: ILVN-2021-0003

CVE-ID: CVE-2021-36718

Affected Products: Synel – eharmonynew / Synel Reports 8.02

Description: Credentials Management Errors - weaknesses in this category are related to the management of credentials. The attacker can log in to the system with default credentials and export reports of eharmony system with sensitive data (employee name, employee ID, working hours etc').

Solution: Update to – eharmonynew version 11

Credit/Acknowledgments: Dudu Moyal , Sophtix

Public Date: 15/11/202

Synerion - Directory Traversal

ILVN-ID: ILVN-2021-0002

CVE-ID: CVE-2021-36717

Affected Products: TimeNet version 9.21

Description: Directory Traversal - is an attack against a server or a Web application aimed at unauthorized access to the file system. on the "Name" parameter the attacker can return to the root directory and open the host file.

This might give the attacker the ability to view restricted files, which could provide the attacker with more information required to further compromise the system.

Credit/Acknowledgments: Gad Abuhatziera , Sophtix

Public Date: 01/09/2021

CyberArk Identity - Username Enumeration

ILVN-ID: ILVN-2021-0001

CVE-ID: CVE-2021-37151

Affected Products: CyberArk Identity 21.5.131

Description: With certain authentication policy configurations, it might appear that the API response length can be used to differentiate between a valid user and an invalid one.

Solution: For an end user, to prevent differentiation between responses of invalid users vs valid users is to fill out all of the possible MFA options that are enabled for that user. For an admin setting up the policy, a good way to prevent differentiation is to make sure to enable MFA options that you expect the majority of your userbase to have. Having your userbase use for example, only password as a first challenge and only FIDO2 compatible factor as a second challenge for the "Everybody" role can be a great way to set up secure MFA for your users.

Credit/Acknowledgments: Eli Goldiner

Public Date: 22/08/2021

More on the subject

Vulnerability Reporting Form