BOLETIM DE VULNERABILIDADES SEMANAL

Esse boletim informa todas as vulnerabilidades de severidades crítica e alta que foram publicadas nesta semana, alertando sobre os novos riscos que podem impactar o seu negócio.

Nesta semana foram detectadas:

VULNERABILIDADES DE SEVERIDADE CRÍTICA

VULNERABILIDADES DE SEVERIDADE ALTA

Scaneie ou clique para falar com nossos especialistas e descobrir se você está vulnerável

IBLISS DIGITAL SECURITY

VULNERABILIDADES DE SEVERIDADE CRÍTICA

ID	CVSS Score	Descrição	Publicado em
CVE-2022-29842	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability that could allow an attacker to execute code in the context of the root user on a vulnerable CGI file was discovered in Western Digital My Cloud OS 5 devicesThis issue affects My Cloud OS 5: before 5.26.119	10/05/2023 21h15
CVE-2023-30194	9.8	Prestashop posstaticfooter <= 1.0.0 is vulnerable to SQL Injection via posstaticfooter::getPosCurrentHook	10/05/2023 20h15
CVE-2023-30189	9.8	Prestashop posstaticblocks <= 1.0.0 is vulnerable to SQL Injection via posstaticblocks::getPosCurrentHook()	16/05/2023 20h15
CVE-2023-2645	9.8	A vulnerability, which was classified as critical, was found in USR USR-G806 1.0.41. Affected is an unknown function of the component Web Management Page. The manipulation of the argument username/password with the input root leads to use of hard-coded password. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to change the configuration settings. VDB-228774 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way	11/05/2023 15h08

#porumasociedademaissegura

IBLISS DIGITAL SECURITY

CVE-2023-0851	9.8	Buffer overflow in CPCA Resource Download process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe	11/05/2023 13h15
CVE-2023-0852	9.8	Buffer overflow in the Address Book of Mobile Device function of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe	11/05/2023 13h15
CVE-2023-0853	9.8	'Buffer overflow in mDNS NSEC record registering process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	11/05/2023 13h15
CVE-2023-0854	9.8	Buffer overflow in NetBIOS QNAME registering and communication process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	11/05/2023 13h15
CVE-2023-0855	9.8	Buffer overflow in IPP number-up attribute process of Office / Small Office Multifunction Printers and Laser Printers(*) which may allow an attacker on the network segment to trigger the affected product being unresponsive or to execute arbitrary code. *:Satera LBP660C Series/LBP620C Series/MF740C Series/MF640C Series firmware Ver.11.04 and earlier sold in Japan. Color imageCLASS LBP660C Series/LBP 620C Series/X LBP1127C/MF740C Series/MF640C Series/X MF1127C firmware Ver.11.04 and earlier sold in US. i-SENSYS LBP660C Series/LBP620C Series/MF740C Series/MF640C Series, C1127P, C1127iF, C1127i firmware Ver.11.04 and earlier sold in Europe.	11/05/2023 13h15

CVE-2023-0856	9.8	The RegistrationMagic plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.2.1.0. This is due to insufficient verification on the user being supplied during a Google social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email	11/05/2023 13h15
CVE-2023-1834	9.4	Rockwell Automation was made aware that Kinetix 5500 drives, manufactured between May 2022 and January 2023, and are running v7.13 may have the telnet and FTP ports open by default. This could potentially allow attackers unauthorized access to the device through the open ports	11/05/2023 19h15
CVE-2023-31148	9.1	An Improper Input Validation vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) Web Interface could allow a remote authenticated attacker to execute arbitrary code. See SEL Service Bulletin dated 2022-11-15 for more details.	10/05/2023 20h15
CVE-2023-32070	9.0	XWiki Platform is a generic wiki platform. Prior to version 14.6-rc-1, HTML rendering didn't check for dangerous attributes/attribute values. This allowed cross-site scripting (XSS) attacks via attributes and link URLs, e.g., supported in XWiki syntax. This has been patched in XWiki 14.6-rc-1. There are no known workarounds apart from upgrading to a fixed version	10/05/2023 18h15
CVE-2023-1698	9.0	Wings is the server control plane for Pterodactyl Panel. A vulnerability affecting versions prior to 1.7.5 and versions 1.11.0 prior to 1.11.6 impacts anyone running the affected versions of Wings. This vulnerability can be used to gain access to the host system running Wings if a user is able to modify an server's install script or the install script executes code supplied by the user (either through environment variables, or commands that execute commands based off of user data). This vulnerability has been resolved in version 'v1.11.6' of Wings, and has been back-ported to the 1.7 release series in 'v1.7.5'. Anyone running 'v1.11.x' should upgrade to 'v1.11.6' and anyone running 'v1.7.x' should upgrade to 'v1.7.5'. There are no workarounds aside from upgrading. Running Wings with a rootless container runtime may mitigate the severity of any attacks, however the majority of users are using container runtimes that run as root as per the Wings documentation. SELinux may prevent attackers from performing certain operations against the host system, however privileged containers have a lot of freedom even on systems with SELinux enabled. It should be noted that this was a known attack vector, for attackers to easily exploit this attack it would require compromising an administrator account on a Panel. However, certain eggs (the data structure that holds the install scripts that get passed to Wings) have an issue where they are unknowingly executing shell commands with escalated privileges provided by untrusted user data	10/05/2023 21h15

VULNERABILIDADES DE SEVERIDADE ALTA

ID	CVSS Score	Descrição	Publicado em
CVE-2022-45846	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Nickys Image Map Pro for WordPress - Interactive SVG Image Map Builder plugin 5.6.9 versions	10/05/2023 12h15
CVE-2022-41784	8.8	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-27298	8.8	Uncontrolled search path in the WULT software maintained by Intel(R) before version 1.0.0 (commit id 592300b) may allow an unauthenticated user to potentially enable escalation of privilege via network access	10/05/2023 14h15
CVE-2023-28410	8.8	Improper restriction of operations within the bounds of a memory buffer in some Intel(R) i915 Graphics drivers for linux before kernel version 6.2.10 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-31566	8.8	Podofo v0.10.0 was discovered to contain a heap-use-after-free via the component PoDoFo::PdfEncrypt::IsMetadataEncrypted()	10/05/2023 16h15
CVE-2023-31567	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptAESV3::PdfEncryptAESV3	10/05/2023 16h15

CVE-2023-31568	8.8	Podofo v0.10.0 was discovered to contain a heap buffer overflow via the component PoDoFo::PdfEncryptRC4::PdfEncryptRC4	10/05/2023 16h15
CVE-2023-2674	8.8	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1	12/05/2023 08h15
CVE-2023-32073	8.8	WWBN AVideo is an open source video platform. In versions 12.4 and prior, a command injection vulnerability exists at 'plugin/CloneSite/cloneClient.json.php' which allows Remote Code Execution if you CloneSite Plugin. This is a bypass to the fix for CVE-2023-30854, which affects WWBN AVideo up to version 12.3. This issue is patched in commit 1df4af01f80d56ff2c4c43b89d0bac151e7fb6e3	12/05/2023 14h15
CVE-2023-32305	8.8	aiven-extras is a PostgreSQL extension. Versions prior to 1.1.9 contain a privilege escalation vulnerability, allowing elevation to superuser inside PostgreSQL databases that use the aiven-extras package. The vulnerability leverages missing schema qualifiers on privileged functions called by the aiven-extras extension. A low privileged user can create objects that collide with existing function names, which will then be executed instead. Exploiting this vulnerability could allow a low privileged user to acquire 'superuser' privileges, which would allow full, unrestricted access to all data and database functions. And could lead to arbitrary code execution or data access on the underlying host as the 'postgres' user. The issue has been patched as of version 1.1.9	12/05/2023 19h15
CVE-2023-32306	8.8	Time Tracker is an open source time tracking system. A time-based blind injection vulnerability existed in Time Tracker reports in versions prior to 1.22.13.5792. This was happening because the 'reports.php' page was not validating all parameters in POST requests. Because some parameters were not checked, it was possible to craft POST requests with malicious SQL for Time Tracker database. This issue is fixed in version 1.22.13.5792. As a workaround, use the fixed code in 'ttReportHelper.class.php' from version 1.22.13.5792.	12/05/2023 19h15
CVE-2022-47379	8.8	An authenticated, remote attacker may use a out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into memory which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47380	8.8	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47381	8.8	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15

CVE-2022-47382	8.8	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47383	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47384	8.8	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47385	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpAppForce Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47386	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47387	8.8	An authenticated remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47388	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47389	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15
CVE-2022-47390	8.8	An authenticated, remote attacker may use a stack based out-of-bounds write vulnerability in the CmpTraceMgr Component of multiple CODESYS products in multiple versions to write data into the stack which can lead to a denial-of-service condition, memory overwriting, or remote code execution	15/05/2023 10h15

CVE-2022-41985	8.6	An authentication bypass vulnerability exists in the Authentication functionality of Weston Embedded uC-FTPs v 1.98.00. A specially crafted set of network packets can lead to authentication bypass and denial of service. An attacker can send a sequence of unauthenticated packets to trigger this vulnerability	10/05/2023 16h15
CVE-2022-21804	8.4	Out-of-bounds write in software for the Intel QAT Driver for Windows before version 1.9.0-0008 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-31208	8.3	Improper neutralization of livestatus command delimiters in the RestAPI in Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users	17/05/2023 09h15
CVE-2022-40207	8.2	Improper access control in the Intel(R) SUR software before version 2.4.8989 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-41699	8.2	Incorrect permission assignment for critical resource in some Intel(R) QAT drivers for Windows before version 1.9.0 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-44619	8.2	Insecure storage of sensitive information in the Intel(R) DCM software before version 5.1 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-22297	8.2	Access of memory location after end of buffer in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-22661	8.2	Buffer overflow in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-25545	8.2	Improper buffer restrictions in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-25568	8.2	Boxo, formerly known as go-libipfs, is a library for building IPFS applications and implementations. In versions 0.4.0 and 0.5.0, if an attacker is able allocate arbitrary many bytes in the Bitswap server, those allocations are lasting even if the connection is closed. This affects users accepting untrusted connections with the Bitswap server and also affects users using the old API stubs at 'github.com/ipfs/go-libipfs/bitswap' because users then transitively import 'github.com/ipfs/go-libipfs/bitswap/server'. Boxo versions 0.6.0 and 0.4.1 contain a patch for this issue. As a workaround, those who are using the stub object at 'github.com/ipfs/go-libipfs/bitswap' not taking advantage of the features provided by the server can refactor their code to use the new split API that will allow them to run in a client only mode: 'github.com/ipfs/go-libipfs/bitswap/client'	10/05/2023 14h15

CVE-2023-32308	8.2	anuko timetracker is an open source time tracking system. Boolean-based blind SQL injection vulnerability existed in Time Tracker invoices.php in versions prior to 1.22.11.5781. This was happening because of a coding error after validating parameters in POST requests. There was no check for errors before adjusting invoice sorting order. Because of this, it was possible to craft a POST request with malicious SQL for Time Tracker database. This issue has been fixed in version 1.22.11.5781. Users are advised to upgrade. Users unable to upgrade may insert an additional check for errors in a condition before calling 'ttGroupHelper::getActiveInvoices()' in invoices.php	15/05/2023 21h15
CVE-2023-32955	8.1	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DHCP Client Functionality in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows man-in-the-middle attackers to execute arbitrary commands via unspecified vectors	16/05/2023 08h15
CVE-2023-2706	8.1	The OTP Login Woocommerce & Gravity Forms plugin for WordPress is vulnerable to authentication bypass. This is due to the fact that when generating OTP codes for users to use in order to login via phone number, the plugin returns these codes in an AJAX response. This makes it possible for unauthenticated attackers to obtain login codes for administrators. This does require an attacker have access to the phone number configured for an account, which can be obtained via social engineering or reconnaissance	17/05/2023 02h15
CVE-2023-31150	8.0	A Storing Passwords in a Recoverable Format vulnerability in the Schweitzer Engineering Laboratories Real-Time Automation Controller (SEL RTAC) database system could allow an authenticated attacker to retrieve passwords. See SEL Service Bulletin dated 2022-11-15 for more details	10/05/2023 20h15
CVE-2022-29841	8.0	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that was caused by a command that read files from a privileged location and created a system command without sanitizing the read data. This command could be triggered by an attacker remotely to cause code execution and gain a reverse shell in Western Digital My Cloud OS 5 devices.This issue affects My Cloud OS 5: before 5.26.119	10/05/2023 22h15
CVE-2023-22442	7.9	Out of bounds write in some Intel(R) Server Board BMC firmware before version 2.90 may allow a privileged user to enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-29919	7.8	Use after free in the Intel(R) VROC software before version 7.7.6.1003 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-23569	7.8	Stack-based buffer overflow for some Intel(R) Trace Analyzer and Collector software before version 2021.8.0 published Dec 2022 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-31906	7.8	Jerryscript 3.0.0(commit 1a2c047) was discovered to contain a heap-buffer-overflow via the component lexer_compare_identifier_to_chars at /jerry-core/parser/js/js-lexer.c	10/05/2023 15h15

CVE-2023-31907	7.8	Jerryscript 3.0.0 was discovered to contain a heap-buffer-overflow via the component scanner_literal_is_created at /jerry-core/parser/js/js-scanner-util.c	10/05/2023 15h15
CVE-2023-29273	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29276	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29278	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29280	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29282	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29283	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-29285	7.8	Adobe Substance 3D Painter versions 8.3.0 (and earlier) is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file	11/05/2023 22h15
CVE-2023-30768	7.7	Improper access control in the Intel(R) Server Board S2600WTT belonging to the Intel(R) Server Board S2600WT Family with the BIOS version 0016 may allow a privileged user to potentially enable escalation of privilege via local access	12/05/2023 15h15
CVE-2023-31199	7.7	Improper access control in the Intel(R) Solid State Drive Toolbox(TM) before version 3.4.5 may allow a privileged user to potentially enable escalation of privilege via local access	12/05/2023 15h15
CVE-2022-4048	7.7	Inadequate Encryption Strength in CODESYS Development System V3 versions prior to V3.5.18.40 allows an unauthenticated local attacker to access and manipulate code of the encrypted boot application	15/05/2023 10h15

CVE-2022-28699	7.5	Improper input validation for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-33894	7.5	Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-34147	7.5	Improper input validation in BIOS firmware for some Intel(R) NUC 9 Extreme Laptop Kits, Intel(R) NUC Performance Kits, Intel(R) NUC Performance Mini PC, Intel(R) NUC 8 Compute Element, Intel(R) NUC Pro Kit, Intel(R) NUC Pro Board, and Intel(R) NUC Compute Element may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-36339	7.5	Improper input validation in firmware for Intel(R) NUC 8 Compute Element, Intel(R) NUC 11 Compute Element, Intel(R) NUC 12 Compute Element may allow a privileged user to enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-43507	7.5	Improper buffer restrictions in the Intel(R) QAT Engine for OpenSSL before version 0.6.16 may allow a privileged user to potentially enable escalation of privilege via network access	10/05/2023 14h15
CVE-2023-2443	7.5	Automation ThinManager product allows the use of medium strength ciphers. If the client requests an insecure cipher, a malicious actor could potentially decrypt traffic sent between the client and server API	11/05/2023 19h15
CVE-2023-31146	7.5	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, during codegen, the length word of a dynarray is written before the data, which can result in out-of-bounds array access in the case where the dynarray is on both the lhs and rhs of an assignment. The issue can cause data corruption across call frames. The expected behavior is to revert due to out-of-bounds array access. Version 0.3.8 contains a patch for this issue	11/05/2023 21h15
CVE-2023-32058	7.5	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, due to missing overflow check for loop variables, by assigning the iterator of a loop to a variable, it is possible to overflow the type of the latter. The issue seems to happen only in loops of type 'for i in range(a, a + N)' as in loops of type 'for i in range(start, stop)' and 'for i in range(stop)', the compiler is able to raise a 'TypeMismatch' when trying to overflow the variable. The problem has been patched in version 0.3.8	11/05/2023 21h15
CVE-2023-32059	7.5	Vyper is a Pythonic smart contract language for the Ethereum virtual machine. Prior to version 0.3.8, internal calls with default arguments are compiled incorrectly. Depending on the number of arguments provided in the call, the defaults are added not right-to-left, but left-to-right. If the types are incompatible, typechecking is bypassed. The ability to pass kwargs to internal functions is an undocumented feature that is not well known about. The issue is patched in version 0.3.8	12/05/2023 15h15
CVE-2023-2665	7.5	Storage of Sensitive Data in a Mechanism without Access Control in GitHub repository francoisjacquet/rosariosis prior to 11.0	12/05/2023 01h15

CVE-2023-23444	7.5	Missing Authentication for Critical Function in SICK Flexi Classic and Flexi Soft Gateways with Partnumbers 1042193, 1042964, 1044078, 1044072, 1044073, 1044074, 1099830, 1099832, 1127717, 1069070, 1112296, 1051432, 1102420, 1127487, 1121596, 1121597 allows an unauthenticated remote attacker to influence the availability of the device by changing the IP settings of the device via broadcasted UDP packets	12/05/2023 13h15
CVE-2023-22318	7.5	Denial of service in Webconf in Tribe29 Checkmk Appliance before 1.6.5	15/05/2023 09h15
CVE-2022-47391	7.5	In multiple CODESYS products in multiple versions an unauthorized, remote attacker may use a improper input validation vulnerability to read from invalid addresses leading to a denial of service	15/05/2023 10h15
CVE-2022-36339	7.5	Improper Access Control in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to gain unauthorized access to data fields by using a therefore unpriviledged account via the REST interface	15/05/2023 11h15
CVE-2023-23447	7.5	Uncontrolled Resource Consumption in SICK FTMg AIR FLOW SENSOR with Partnumbers 1100214, 1100215, 1100216, 1120114, 1120116, 1122524, 1122526 allows an unprivileged remote attacker to influence the availability of the webserver by invocing several open file requests via the REST interface	15/05/2023 11h15
CVE-2023-32309	7.5	PyMdown Extensions is a set of extensions for the `Python-Markdown` markdown project. In affected versions an arbitrary file read is possible when using include file syntax. By using the syntax `--8<--"/etc/passwd"` or `--8<--"/proc/self/environ"` the content of these files will be rendered in the generated documentation. Additionally, a path relative to a specified, allowed base path can also be used to render the content of a file outside the specified base paths: `--8<-- "../../../../etc/passwd"`. Within the Snippets extension, there exists a `base_path` option but the implementation is vulnerable to Directory Traversal. The vulnerable section exists in `get_snippet_path(self, path)` lines 155 to 174 in snippets.py. Any readable file on the host where the plugin is executing may have its content exposed. This can impact any use of Snippets that exposes the use of Snippets to external users. It is never recommended to use Snippets to process user-facing, dynamic content. It is designed to process known content on the backend under the control of the host, but if someone were to accidentally enable it for user-facing content, undesired information could be exposed. This issue has been addressed in version 10.0. Users are advised to upgrade. Users unable to upgrade may restrict relative paths by filtering input	15/05/2023 21h15
CVE-2023-31131	7.4	Greenplum Database (GPDB) is an open source data warehouse based on PostgreSQL. In versions prior to 6.22.3 Greenplum Database used an unsafe methods to extract tar files within GPPKGs. greenplum-db is vulnerable to path traversal leading to arbitrary file writes. An attacker can use this vulnerability to overwrite data or system files potentially leading to crash or malfunction of the system. Any files which are accessible to the running process are at risk. All users are requested to upgrade to Greenplum Database version 6.23.2 or higher. There are no known workarounds for this vulnerability	15/05/2023 22h15

CVE-2023-2641	7.3	A vulnerability was found in SourceCodester Online Internship Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/login.php of the component POST Parameter Handler. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-228770 is the identifier assigned to this vulnerability	11/05/2023 06h15
CVE-2022-32766	7.2	Improper input validation for some Intel(R) BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2022-42465	7.2	Improper access control in kernel mode driver for the Intel(R) OFU software before version 14.1.30 may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-22312	7.2	Improper access control for some Intel(R) NUC BIOS firmware may allow a privileged user to potentially enable escalation of privilege via local access	10/05/2023 14h15
CVE-2023-2649	7.2	A vulnerability was found in Tenda AC23 16.03.07.45_cn. It has been declared as critical. This vulnerability affects unknown code of the file /bin/ate of the component Service Port 7329. The manipulation of the argument v2 leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-228778 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way	11/05/2023 08h15
CVE-2023-30763	7.2	Heap-based overflow in Intel(R) SoC Watch based software before version 2021.1 may allow a privileged user to potentially enable escalation of privilege via local access	12/05/2023 15h15
CVE-2023-30501	7.2	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise	16/05/2023 19h15
CVE-2023-30502	7.2	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise	16/05/2023 19h15
CVE-2023-2753	7.2	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta	17/05/2023 08h15
CVE-2022-41690	7.1	mproper access control in the Intel(R) Retail Edge Mobile iOS application before version 3.4.7 may allow an authenticated user to potentially enable escalation of privilege via local access	10/05/2023 14h15

CVE-2023-29030	7.1	A cross site scripting vulnerability was discovered in Rockwell Automation's ArmorStart ST product that could potentially allow a malicious user to view and modify sensitive data or make the web page unavailable. User interaction, such as a phishing attack, is required for successful exploitation of this vulnerability	11/05/2023 18h15
CVE-2023-2444	7.1	A cross site request forgery vulnerability exists in Rockwell Automation's FactoryTalk Vantagepoint. This vulnerability can be exploited in two ways. If an attacker sends a malicious link to a computer that is on the same domain as the FactoryTalk Vantagepoint server and a user clicks the link, the attacker could impersonate the legitimate user and send requests to the affected product. Additionally, if an attacker sends an untrusted link to a computer that is not on the same domain as the server and a user opens the FactoryTalk Vantagepoint website, enters credentials for the FactoryTalk Vantagepoint server, and clicks on the malicious link a cross site request forgery attack would be successful as well	11/05/2023 19h15
CVE-2023-22703	7.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Webcodin WCP Contact Form plugin <= 3.1.0 versions	15/05/2023 11h15
CVE-2023-22706	7.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in PropertyHive plugin <= 1.5.48 versions	15/05/2023 12h15
CVE-2023-29439	7.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FooPlugins FooGallery plugin <= 2.2.35 versions	16/05/2023 15h15
CVE-2023-2509	7.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below	17/05/2023 07h15
CVE-2023-0864	7.1	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5	17/05/2023 08h15
CVE-2023-30502	7.1	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise	16/05/2023 19h15

SUA EMPRESA ESTÁ VULNERÁVEL?

Uma empresa pode levar até 12 horas para identificar uma vulnerabilidade grave por não ter visibilidade de seus ativos, o que pode gerar inúmeros prejuízos financeiros.

Com um time de especialistas altamente certificados, nosso Programa de Consultoria em Cibersegurança foi desenhado para uma rápida detecção e resposta a incidentes, aumentando a visão e diminuindo os riscos em seu ambiente organizacional.

Scaneie ou clique para falar com nossos especialistas e descubra como se proteger

#porumasociedademaissegura

IBLISS
DIGITAL SECURITY