Newsletter on system vulnerabilities and cybersecurity news.

National Cyber Security Authority (NCSA)

Date: 08/04/2025 - 11/04/2025

Contents

Common Vulnerabilities and Exposures (CVEs)

URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/Εκδόσεις που επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-41794	10	SENTRON 7KT PAC1260 Data Manager	Use of Hard-coded Credentials	SENTRON 7KT PAC1260 Data Manager (All versions)	https://cert-portal.siemens.com/productcert/html/ssa-187636.html
https://nvd.nist.gov/vuln/detail/CVE-2025-31330	9,9	SAP Landscape Transformation (SLT)	Improper Control of Generation of Code ('Code Injection')		https://me.sap.com/notes/3587115 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2024-48887	9,8	Fortinet FortiSwitch GUI	Unverified Password Change	A unverified password change vulnerability in Fortinet FortiSwitch GUI may allow a remote unauthenticated attacker to change admin passwords via a specially crafted request	https://fortiguard.fortinet.com/psirt/FG-IR-24-435
https://nvd.nist.gov/vuln/detail/CVE-2025-29087	9,8	Sqlite	Integer Overflow or Wraparound	Sqlite 3.49.0 is susceptible to integer overflow through the concat function	https://gist.github.com/ylwango613/a44a29f1ef074fa783e29f04a0afd62a
https://nvd.nist.gov/vuln/detail/CVE-2025-30282	9,1	ColdFusion	Improper Authentication	ColdFusion versions 2023.12, 2021.18, 2025.0 and earlier	https://helpx.adobe.com/security/products/coldfusion/apsb25-15.html

https://nvd.nist.gov/vuln/detail/CVE-2025-20946	8,8	Galaxy Watch Bluetooth	CWE	Galaxy Watch Bluetooth pairing prior to SMR Apr-2025 Release 1	https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=04
https://nvd.nist.gov/vuln/detail/CVE-2025-1095	8,8	IBM Personal Communications	Improper Restriction of Operations within the Bounds of a Memory Buffer	IBM Personal Communications v14 and v15	https://www.ibm.com/support/pages/node/7230335
https://nvd.nist.gov/vuln/detail/CVE-2025-29794	8,8	Microsoft Office SharePoint	Improper Authorization	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29794
https://nvd.nist.gov/vuln/detail/CVE-2025-27740	8,8	Windows Active Directory Certificate Services	Weak Authentication	Weak authentication in Windows Active Directory Certificate Services allows an authorized attacker to elevate privileges over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27740
https://nvd.nist.gov/vuln/detail/CVE-2025-26669	8,8	Windows Routing and Remote Access Service (RRAS)	Out-of-bounds Read	Out-of-bounds read in Windows Routing and Remote Access Service (RRAS) allows an unauthorized attacker to disclose information over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26669
https://nvd.nist.gov/vuln/detail/CVE-2025-27481	8,8	Windows Telephony Service	Stack-based Buffer Overflow	Stack-based buffer overflow in Windows Telephony Service allows an unauthorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27481

https://nvd.nist.gov/vuln/detail/CVE-2024-12556	8,7	Prototype Pollution in Kibana	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')		https://discuss.elastic.co/t/kibana-8-16-4-and-8-17-2-security-update-esa-2025-02/376918
https://nvd.nist.gov/vuln/detail/CVE-2025-32406	8,6	NAKIVO Backup & Replication	Improper Restriction of XML External Entity Reference	NAKIVO Backup & Replication 10.3.x through 11.0.1 before 11.0.2	https://helpcenter.nakivo.com/KnowledgeBase/Content/Security-Advisory/CVE-2025-32406.htm
https://nvd.nist.gov/vuln/detail/CVE-2025-27737	8,6	Windows Security Zone Mapping	Improper Input Validation	Improper input validation in Windows Security Zone Mapping allows an unauthorized attacker to bypass a security feature locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27737
https://nvd.nist.gov/vuln/detail/CVE-2025-23186	8,5	SAP NetWeaver Application Server ABAP	Improper Control of Generation of Code ('Code Injection')	SAP NetWeaver Application Server ABAP	https://me.sap.com/notes/3554667 https://url.sap/sapsecuritypatchday
https://nvd.nist.gov/vuln/detail/CVE-2025-26678	8,4	Windows Defender Application Control (WDAC)	Improper Access Control	Improper access control in Windows Defender Application Control (WDAC) allows an unauthorized attacker to bypass a security feature locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26678

https://nvd.nist.gov/vuln/detail/CVE-2025-29986	8,3	Dell Common Event Enabler	Improper Restriction of Communication Channel to Intended Endpoints	Dell Common Event Enabler, version(s) CEE 9.0.0.0	https://www.dell.com/support/kbdoc/en-us/000303931/dsa-2025-158-security-update-for-dell-common-event-enabler-vulnerabilities
https://nvd.nist.gov/vuln/detail/CVE-2025-27480	8,1	Remote Desktop Gateway Service	Use After Free	Use after free in Remote Desktop Gateway Service allows an unauthorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27480
https://nvd.nist.gov/vuln/detail/CVE-2025-26671	8,1	Windows Remote Desktop Services	Use After Free	Use after free in Windows Remote Desktop Services allows an unauthorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26671
https://nvd.nist.gov/vuln/detail/CVE-2025-30285	8	ColdFusion	Deserialization of Untrusted Data	ColdFusion versions 2023.12, 2021.18, 2025.0	https://helpx.adobe.com/security/products/coldfusion/apsb25-15.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27487	8	Remote Desktop Client	Heap-based Buffer Overflow	Heap-based buffer overflow in Remote Desktop Client allows an authorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27487
https://nvd.nist.gov/vuln/detail/CVE-2025-30304	7,8	Adobe Framemaker	Out-of-bounds Write	Adobe Framemaker versions 2020.8, 2022.6 and earlier	https://helpx.adobe.com/security/products/framemaker/apsb25-33.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27489	7,8	Azure	Improper Input Validation	Improper input validation in Azure Local allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27489

https://nvd.nist.gov/vuln/detail/CVE-2025-27193	7,8	Bridge	Heap-based Buffer Overflow	Bridge versions 14.1.5, 15.0.2 and earlier	https://helpx.adobe.com/security/products/bridge/apsb25-25.html
https://nvd.nist.gov/vuln/detail/CVE-2025-29800	7,8	Microsoft AutoUpdate (MAU)	Improper Privilege Management	Improper privilege management in Microsoft AutoUpdate (MAU) allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29800
https://nvd.nist.gov/vuln/detail/CVE-2025-29791	7,8	Microsoft Office	Access of Resource Using Incompatible Type ('Type Confusion')	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29791
https://nvd.nist.gov/vuln/detail/CVE-2025-27748	7,8	Microsoft Office	Use After Free	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27748
https://nvd.nist.gov/vuln/detail/CVE-2025-29823	7,8	Microsoft Office Excel	Use After Free	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29823
https://nvd.nist.gov/vuln/detail/CVE-2025-27752	7,8	Microsoft Office Excel	Heap-based Buffer Overflow	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27752
https://nvd.nist.gov/vuln/detail/CVE-2025-29822	7,8	Microsoft Office OneNote	Incomplete List of Disallowed Inputs	Incomplete list of disallowed inputs in Microsoft Office OneNote allows an unauthorized attacker to bypass a security feature locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29822

https://nvd.nist.gov/vuln/detail/CVE-2025-29820	7,8	Microsoft Office Word	Use After Free	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29820
https://nvd.nist.gov/vuln/detail/CVE-2025-26688	7,8	Microsoft Virtual Hard Drive	Stack-based Buffer Overflow	Stack-based buffer overflow in Microsoft Virtual Hard Drive allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26688
https://nvd.nist.gov/vuln/detail/CVE-2025-27731	7,8	OpenSSH	Improper Input Validation	Improper input validation in OpenSSH for Windows allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27731
https://nvd.nist.gov/vuln/detail/CVE-2025-27198	7,8	Photoshop	Heap-based Buffer Overflow	Photoshop Desktop versions 25.12.1, 26.4.1 and earlier	https://helpx.adobe.com/security/products/photoshop/apsb25-30.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27196	7,8	Premiere Pro	Heap-based Buffer Overflow	Premiere Pro versions 25.1, 24.6.4 and earlier	https://helpx.adobe.com/security/products/premiere_pro/apsb25-28.html
https://nvd.nist.gov/vuln/detail/CVE-2025-27730	7,8	Windows Digital Media	Double Free	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27730
https://nvd.nist.gov/vuln/detail/CVE-2025-27476	7,8	Windows Digital Media	Use After Free	Use after free in Windows Digital Media allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27476
https://nvd.nist.gov/vuln/detail/CVE-2025-24060	7,8	Windows DWM Core Library	Improper Input Validation	Improper input validation in Windows DWM Core Library allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24060

https://nvd.nist.gov/vuln/detail/CVE-2025-27727	7,8	Windows Installer	Improper Link Resolution Before File Access ('Link Following')	Improper link resolution before file access ('link following') in Windows Installer allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27727
https://nvd.nist.gov/vuln/detail/CVE-2025-26648	7,8	Windows Kernel	Use After Free	Sensitive data storage in improperly locked memory in Windows Kernel allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26648
https://nvd.nist.gov/vuln/detail/CVE-2025-29812	7,8	Windows Kernel Memory	Untrusted Pointer Dereference	Untrusted pointer dereference in Windows Kernel Memory allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29812
https://nvd.nist.gov/vuln/detail/CVE-2025-27728	7,8	Windows Kernel-Mode Drivers	Out-of-bounds Read	Out-of-bounds read in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27728
https://nvd.nist.gov/vuln/detail/CVE-2025-29811	7,8	Windows Mobile Broadband	Improper Input Validation	Improper input validation in Windows Mobile Broadband allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29811
https://nvd.nist.gov/vuln/detail/CVE-2025-27741	7,8	Windows NTFS	Out-of-bounds Read	Out-of-bounds read in Windows NTFS allows an unauthorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27741
https://nvd.nist.gov/vuln/detail/CVE-2025-27729	7,8	Windows Shell	Use After Free	Use after free in Windows Shell allows an unauthorized attacker to execute code locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27729

https://nvd.nist.gov/vuln/detail/CVE-2025-26675	7,8	Windows Subsystem for Linux	Out-of-bounds Read	Out-of-bounds read in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26675
https://nvd.nist.gov/vuln/detail/CVE-2025-26639	7,8	Windows USB Print Driver	Heap-based Buffer Overflow	Integer overflow or wrap-around in Windows USB Print Driver allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26639
https://nvd.nist.gov/vuln/detail/CVE-2025-29810	7,5	Active Directory Domain Services	Improper Access Control	Improper access control in Active Directory Domain Services allows an authorized attacker to elevate privileges over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29810
https://nvd.nist.gov/vuln/detail/CVE-2025-32031	7,5	Apollo Gateway	Allocation of Resources Without Limits or Throttling	Prior to 2.10.1, a vulnerability in Apollo Gateway	https://github.com/apollographql/federation/pull/3236 https://github.com/apollographql/federation/releases/tag/%40apollo%2Fgateway%402.10.1 https://github.com/apollographql/federation/security/advisories/GHSA-p2q6-pwh5-m6jr`
https://nvd.nist.gov/vuln/detail/CVE-2025-32033	7,5	Apollo Router Core	Improper Restriction of Operations within the Bounds of a Memory Buffer	Apollo Federation 2. Prior to 1.61.2 and 2.1.1	https://github.com/apollographql/router/commit/ab6675a63174715ea6ff50881fc957831d4e9564 https://github.com/apollographql/router/commit/bba032e183b861348a466d3123c7137a1ae18952 https://github.com/apollographql/router/security/advisories/GHSA-84m6-5m72-45fp

https://nvd.nist.gov/vuln/detail/CVE-2023-37930	7,5	Fortinet FortiOS SSL VPN webmode	Use of Uninitialized Resource	Fortinet FortiOS SSL VPN webmode version 7.4.0, version 7.2.0 through 7.2.5, version 7.0.1 through 7.0.11 and version 6.4.7 through 6.4.14 and Fortinet FortiProxy SSL VPN webmode version 7.2.0 through 7.2.6 and version 7.0.0 through 7.0.12	https://fortiguard.com/psirt/FG-IR-23-165
https://nvd.nist.gov/vuln/detail/CVE-2025-25227	7,5	Joomla CMS	Improper Authentication	Joomla CMS Multi-Factor Authentication	https://developer.joomla.org/security-centre/964-20250402-core-mfa-authentication-bypass.html
https://nvd.nist.gov/vuln/detail/CVE-2025-21594	7,5	Juniper Networks Junos OS	Improper Check for Unusual or Exceptional Conditions	from 21.2 before 21.2R3-S8, * from 21.4 before 21.4R3-S7, * from 22.1 before 22.1R3-S6, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S3, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R1-S2, 23.4R2. This issue does not affect versions before 20.2R1	https://supportportal.juniper.net/JSA96449
https://nvd.nist.gov/vuln/detail/CVE-2025-29816	7,5	Microsoft Office Word	Acceptance of Extraneous Untrusted Data With Trusted Data	Improper input validation in Microsoft Office Word allows an unauthorized attacker to bypass a security feature over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29816

https://nvd.nist.gov/vuln/detail/CVE-2025-29805	7,5	Outlook for Android	Exposure of Sensitive Information to an Unauthorized Actor	Exposure of sensitive information to an unauthorized actor in Outlook for Android allows an unauthorized attacker to disclose information over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29805
https://nvd.nist.gov/vuln/detail/CVE-2025-26641	7,5	Windows Cryptographic Services	Uncontrolled Resource Consumption	Uncontrolled resource consumption in Windows Cryptographic Services allows an unauthorized attacker to deny service over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26641
https://nvd.nist.gov/vuln/detail/CVE-2025-27473	7,5	Windows HTTP.sys	Uncontrolled Resource Consumption	Uncontrolled resource consumption in Windows HTTP.sys allows an unauthorized attacker to deny service over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27473
https://nvd.nist.gov/vuln/detail/CVE-2025-27479	7,5	Windows Kerberos	Insufficient Resource Pool	Insufficient resource pool in Windows Kerberos allows an unauthorized attacker to deny service over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27479
https://nvd.nist.gov/vuln/detail/CVE-2025-27469	7,5	Windows LDAP - Lightweight Directory Access Protocol	Uncontrolled Resource Consumption	Uncontrolled resource consumption in Windows LDAP - Lightweight Directory Access Protocol allows an unauthorized attacker to deny service over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27469
https://nvd.nist.gov/vuln/detail/CVE-2025-27486	7,5	Windows Standards-Based Storage Management Service	Uncontrolled Resource Consumption	Windows Standards-Based Storage Management Service	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27486

https://nvd.nist.gov/vuln/detail/CVE-2025-27470	7,5	Windows Standards-Based Storage Management Service	Uncontrolled Resource Consumption	Uncontrolled resource consumption in Windows Standards-Based Storage Management Service allows an unauthorized attacker to deny service over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27470
https://nvd.nist.gov/vuln/detail/CVE-2025-26686	7,5	Windows TCP/IP	Sensitive Data Storage in Improperly Locked Memory	Sensitive data storage in improperly locked memory in Windows TCP/IP allows an unauthorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26686
https://nvd.nist.gov/vuln/detail/CVE-2025-27484	7,5	Windows Universal Plug and Play (UPnP) Device Host	Sensitive Data Storage in Improperly Locked Memory	Windows Universal Plug and Play (UPnP) Device Host	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27484
https://nvd.nist.gov/vuln/detail/CVE-2025-26687	7,5	Windows Win32K - GRFX	Use After Free	Use after free in Windows Win32K - GRFX allows an unauthorized attacker to elevate privileges over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26687

https://nvd.nist.gov/vuln/detail/CVE-2025-3401	7,3	ESAFENET	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	ESAFENET CDG 5.6.3.154.205_20250114	https://github.com/Rain1er/report/blob/main/CDG/Ng%3D%3D.md Exploit Third Party Advisory https://github.com/Rain1er/report/blob/main/CDG/Ng%3D%3D.md Exploit Third Party Advisory https://vuldb.com/?ctiid.303646 Permissions Required Third Party Advisory VDB Entry https://vuldb.com/?id.303646 Third Party Advisory VDB Entry https://vuldb.com/?submit.525612 Third Party Advisory VDB Entry
https://nvd.nist.gov/vuln/detail/CVE-2025-29792	7,3	Microsoft Office	Use After Free	Use after free in Microsoft Office allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29792
https://nvd.nist.gov/vuln/detail/CVE-2025-3380	7,3	PCMan FTP Server	Improper Restriction of Operations within the Bounds of a Memory Buffer	PCMan FTP Server 2.0.7	https://fitoxs.com/exploit/exploit-c926c69a41d2fce207cf3a3b789b7a79.txt https://fitoxs.com/exploit/exploit-c926c69a41d2fce207cf3a3b789b7a79.txt https://vuldb.com/?ctiid.303626 https://vuldb.com/?id.303626 https://vuldb.com/?submit.552342
https://nvd.nist.gov/vuln/detail/CVE-2025-29804	7,3	Visual Studio	Improper Access Control	Improper access control in Visual Studio allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29804
https://nvd.nist.gov/vuln/detail/CVE-2025-29802	7,3	Visual Studio	Uncontrolled Search Path Element	Improper access control in Visual Studio allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29802

https://nvd.nist.gov/vuln/detail/CVE-2025-22461	7,2	Ivanti Endpoint Manager	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	Ivanti Endpoint Manager before version 2024 SU1 or before version 2022 SU7	https://forums.ivanti.com/s/article/Security-Advisory-EPM-April-2025-for-EPM-2024-and-EPM-2022-SU6
https://nvd.nist.gov/vuln/detail/CVE-2025-27491	7,1	Windows Hyper-V	Use After Free	Use after free in Windows Hyper-V allows an authorized attacker to execute code over a network	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27491
https://nvd.nist.gov/vuln/detail/CVE-2025-29809	7,1	Windows Kerberos	Insecure Storage of Sensitive Information	Insecure storage of sensitive information in Windows Kerberos allows an authorized attacker to bypass a security feature locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29809
https://nvd.nist.gov/vuln/detail/CVE-2025-27478	7	Windows Local Security Authority (LSA)	Heap-based Buffer Overflow	Heap-based buffer overflow in Windows Local Security Authority (LSA) allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27478
https://nvd.nist.gov/vuln/detail/CVE-2025-27492	7	Windows Secure Channel	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Secure Channel allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27492

https://nvd.nist.gov/vuln/detail/CVE-2025-27475	7	Windows Update Stack	Sensitive Data Storage in Improperly Locked Memory	Sensitive data storage in improperly locked memory in Windows Update Stack allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27475
https://nvd.nist.gov/vuln/detail/CVE-2025-27732	7	Windows Win32K - GRFX	Sensitive Data Storage in Improperly Locked Memory	Sensitive data storage in improperly locked memory in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27732

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας / Ενημερωτικό / Οδηγίες	URL
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ **CVE-2025-30406 Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability** ▪ **CVE-2025-29824 Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability**	https://www.cisa.gov/news-events/alerts/2025/04/08/cisa-adds-two-known-exploited-vulnerabilities-catalog
CISA Adds Two Known Exploited Vulnerabilities to Catalog	▪ **CVE-2024-53197 Linux Kernel Out-of-Bounds Access Vulnerability** ▪ **CVE-2024-53150 Linux Kernel Out-of-Bounds Read Vulnerability**	https://www.cisa.gov/news-events/alerts/2025/04/09/cisa-adds-two-known-exploited-vulnerabilities-catalog
ABB Arctic Wireless Gateways		https://www.cisa.gov/news-events/ics-advisories/icsa-25-100-09
CISA Releases Ten Industrial Control Systems Advisories	▪ **ICSA-25-100-01 Siemens License Server** ▪ **ICSA-25-100-02 Siemens SIDIS Prime** ▪ **ICSA-25-100-03 Siemens Solid Edge** ▪ **ICSA-25-100-04 Siemens Industrial Edge Devices** ▪ **ICSA-25-100-05 Siemens Insights Hub Private Cloud** ▪ **ICSA-25-100-06 Siemens SENTRON 7KT PAC1260 Data Manager** ▪ **ICSA-25-100-07 Rockwell Automation Arena** ▪ **ICSA-25-100-08 Subnet Solutions PowerSYSTEM Center** ▪ **ICSA-25-100-09 ABB Arctic Wireless Gateways** ▪ **ICSMA-25-100-01 INFINITT Healthcare INFINITT PACS**	https://www.cisa.gov/news-events/alerts/2025/04/10/cisa-releases-ten-industrial-control-systems-advisories

News

Σύντομη περιγραφή / Τίτλος	URL
Microsoft 365 Family Subscriptions Users Hit by Licensing Glitch Denies Services	https://cybersecuritynews.com/microsoft-365-family-subscriptions-users/
Researchers Uncovered Hacking Tools and Techniques Discussed on Russian-Speaking Hacking Forums	https://cybersecuritynews.com/researchers-uncovered-hacking-tools-and-techniques-discussed/
Microsoft Exchange Admin Center Down Globally	https://cybersecuritynews.com/microsoft-exchange-admin-center-down/

Breaches / Compromised / Hacked

Σύντομη περιγραφή / Τίτλος	URL

Vulnerabilities / Flaws / Zero-day

Σύντομη περιγραφή / Τίτλος	URL
Windows Kerberos Vulnerability Let Attackers Bypass Security Features & Access Credentials	https://cybersecuritynews.com/windows-kerberos-vulnerability/
CISA Warns of Microsoft Windows CLFS Vulnerability Exploited in Wild	https://cybersecuritynews.com/cisa-warns-of-microsoft-windows-clfs-vulnerability/
5000+ Exposed Ivanti Connect Secure Devices Vulnerable to RCE Attacks	https://cybersecuritynews.com/5000-exposed-ivanti-connect-secure-devices/
Windows CLFS Zero-Day Vulnerability Actively Exploited by Ransomware Group	https://cybersecuritynews.com/windows-clfs-zero-day-vulnerability-actively-exploited-by-ransomware-group/
Windows Common Log File System 0-Day Vulnerability Exploited in the Wild	https://cybersecuritynews.com/windows-common-log-file-system-0-day/
Fortinet Warns of FortiSwitch Vulnerability Let Attackers Modify Admin Passwords	https://cybersecuritynews.com/fortinet-warns-of-fortiswitch-vulnerability/

Potential threats / Threat intelligence

Σύντομη περιγραφή / Τίτλος	URL
TP-Link IoT Smart Hub Vulnerability Exposes Wi-Fi Credentials	https://cybersecuritynews.com/tp-link-iot-smart-hub-vulnerability/
HollowQuill Malware Attacking Government Agencies Worldwide Via Weaponized PDF Documents	https://cybersecuritynews.com/hollowquill-malware-attacking-government-agencies-worldwide/
SideCopy APT Hackers Mimic as Government Personnel to Deploy Open-Source XenoRAT Tool	https://cybersecuritynews.com/sidecopy-apt-hackers-mimic-as-government-personnel/
Microsoft Identity Web Package Vulnerability Exposes Client Secrets & Certificate Information	https://cybersecuritynews.com/microsoft-identity-web-package-vulnerability/
New Double-Edged Email Attack Stealing Office365 Credentials and Deliver Malware	https://cybersecuritynews.com/new-double-edged-email-attack/
CISA Warns of Linux USB-Audio Driver Out-of-Bounds Vulnerability Exploited in the Wild	https://cybersecuritynews.com/cisa-warns-of-linux-usb-audio-driver-out-of-bounds-vulnerability/
Linux USB Audio Driver Vulnerability Let Attackers Execute Arbitrary Code Via Malicious USB Device	https://cybersecuritynews.com/linux-usb-audio-vulnerability/
Windows Active Directory Domain Vulnerability Let Attackers Escalate Privileges	https://cybersecuritynews.com/windows-active-directory-domain-vulnerability-let-attackers-escalate-privileges/
Hellcat Ransomware Updated It's Arsenal to Attack Government, Education, and Energy Sectors	https://cybersecuritynews.com/hellcat-ransomware-updated-its-arsenal/
Windows Remote Desktop Service Vulnerability Let Attackers Execute Malicious Code Remotely	https://cybersecuritynews.com/windows-remote-desktop-service-vulnerability/

Patches / Updates / Fixes

Σύντομη περιγραφή / Τίτλος	URL
Linux Firewall IPFire 2.29 Released With Support for Post-Quantum Cryptography & Core Updates	https://cybersecuritynews.com/linux-firewall-ipfire-2-29-released-with-support/
OpenSSH 10.0 Released With Protocol Changes & Security Upgrades	https://cybersecuritynews.com/openssh-10-0-released/
VMware Patches Multiple 47 Vulnerabilities VMware Tanzu Greenplum Backup & Components	https://cybersecuritynews.com/vmware-patches-multiple-47-vulnerabilities/
Adobe Security Update – Patch for Multiple Vulnerabilities Across Products	https://cybersecuritynews.com/adobe-security-update-multiple-vulnerabilities/
Microsoft Patch Tuesday April 2025 – 121 Vulnerabilities Fixed Including Actively Exploited Zero-Day	https://cybersecuritynews.com/microsoft-patch-tuesday-april-2025/
Fortinet Addresses Multiple Vulnerabilities in FortiAnalyzer, FortiManager, & Other Products	https://cybersecuritynews.com/fortinet-multiple-vulnerabilities-fortios/
SAP April 2025 Security Update : Critical Code Injection Vulnerabilities Patched	https://cybersecuritynews.com/sap-april-2025-security-update/
OpenSSL 3.5.0 Released with Support for Post-Quantum Cryptography	https://cybersecuritynews.com/openssl-3-5-0-released/
Linux 6.15-rc1 Released With Major Driver Update & Perfomance Boost	https://cybersecuritynews.com/linux-6-15-rc1-released/

Guides / Tools

Σύντομη περιγραφή / Τίτλος	URL
Top 11 Best SysAdmin Tools in 2025	https://cybersecuritynews.com/sysadmin-tools/

References

[1]. Ο βαθμός επικινδυνότητας είναι σύμφωνα με την κλίμακα Common Vulnerability Scoring System (CVSSv3), https://nvd.nist.gov/vuln-metrics/cvss

[2]. Τα CVEs αποτελέσματα που εμφανίζονται στην ενότητα 1 διαθέτουν CVSSv3 score >= 7.0 και έχει γίνει μια επιλογή συστημάτων/υπηρεσιών ανάλογα με το πόσο διαδεδομένα είναι.

[3]. Τα CVEs που αφορούν Wordpress plugins θα εμφανίζονται σε ξεχωριστή ενότητα (1.1) σε περιόδους που η εμφάνισή τους είναι ιδιαίτερα αυξημένη.

Annex – Websites with vendor specific vulnerabilities

Ο πίνακας περιέχει websites από κατασκευαστές που προσφέρουν πληροφορίες σχετικές με ευπάθειες που εμφανίζονται στα προϊόντα τους.

Vendor name / Platform	URL
Wordpress	Wordfence Intelligence Vulnerability Database API https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ Scan your WordPress website, https://wpscan.com/scan/
Oracle	Critical Patch Updates, Security Alerts and Bulletins, https://www.oracle.com/security-alerts/
Fortinet	Fortinet products, https://www.fortiguard.com/psirt
IBM	Security bulletins, https://cloud.ibm.com/status/security Research, Collaborate and Act on threat intelligence, https://exchange.xforce.ibmcloud.com/
MS Windows	The Microsoft Security Response Center (MSRC), https://msrc.microsoft.com/update-guide/
SAP	SAP Security Notes, https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html
Dell	Security Advisories, Notices and Resources, https://www.dell.com/support/security/en-us
HPE	HPE Security Bulletin Library, https://support.hpe.com/connect/s/securitybulletinlibrary Security Bulletins, https://support.hp.com/us-en/security-bulletins
Cisco	Cisco Security Advisories, https://sec.cloudapps.cisco.com/security/center/publicationListing.x
Palo Alto	Palo Alto Networks Security Advisories, https://security.paloaltonetworks.com/
Ivanti	Security Advisory, https://www.ivanti.com/blog/topics/security-advisory
Mozilla	Mozilla Foundation Security Advisories, https://www.mozilla.org/en-US/security/advisories/
Android	Android Security Bulletins, https://source.android.com/docs/security/bulletin/asb-overview
Zyxel	Security Advisories, https://www.zyxel.com/global/en/support/security-advisories
D-Link	Global Security Advisories, Responses, and Notices, https://supportannouncement.us.dlink.com/
Adobe	Security Bulletins and Advisories, https://helpx.adobe.com/security/security-bulletin.html
Siemens	Siemens ProductCERT and Siemens CERT, https://www.siemens.com/global/en/products/services/cert.html
Splunk	Splunk Security Advisories, https://advisory.splunk.com/