

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-20419	10	Cisco Smart Software Manager On-Prem	Unverified Password Change	N/A	N/A	https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/smart-software-manager-satellite/datasheet-c78-734539.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy
https://nvd.nist.gov/vuln/detail/CVE-2024-39915	9.9	Thruk is a multibackend monitoring webinterface	Code Injection	N/A	N/A	https://www.thruk.org/ https://github.com/sni/Thruk/security/advisories/GHSA-r7gx-h738-4w6f
https://nvd.nist.gov/vuln/detail/CVE-2024-20401	9.8	Cisco Secure Email Gateway	Absolute Path Traversal	N/A	N/A	https://www.cisco.com/c/en/us/support/security/email-security-appliance/series.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH
https://nvd.nist.gov/vuln/detail/CVE-2024-21181	9.8	Oracle WebLogic Server	vulnerability can result in takeover of	12.2.1.4.0 and	N/A	https://www.oracle.com/java/weblogic/ https://www.oracle.com/security-

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
			service	14.1.1.0.0		alerts/cpujul2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-22442	9.8	Hewlett Packard Enterprise	bypass authentication	N/A	N/A	https://www.hpe.com/us/en/home.html https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04663en_us&docLocale=en_US
https://nvd.nist.gov/vuln/detail/CVE-2024-6457	9.8	HUSKY – Products Filter Professional for WooCommerce plugin for WordPress	time-based SQL Injection	all versions up to, and including, 1.3.6	N/A	https://wordpress.org/plugins/woocommerce-products-filter/ https://www.wordfence.com/threat-intel/vulnerabilities/id/ecfdf7b1-9bb8-4c1d-a00acale44440cab?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-6744	9.8	SMTP Listener of Secure Email Gateway from Cellopoint	Out-of-bounds Write	N/A	N/A	https://www.cellopoint.com/seg https://www.twcert.org.tw/tw/cp-132-7936-f6381-1.html https://www.twcert.org.tw/en/cp-139-7937-acbb5-2.html
https://nvd.nist.gov/vuln/detail/CVE-2024-39736	9.8	IBM Datacap Navigator	Improper Encoding or Escaping of	9.1.5, 9.1.6, 9.1.7, 9.1.8,	N/A	https://www.ibm.com/docs/en/datacap/9.1.8?topic=environment-installing-configuring-datacap-navigator

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
			Output	and 9.1.9		https://www.ibm.com/support/pages/node/7160185
https://nvd.nist.gov/vuln/detail/CVE-2024-39914	9.8	FOG is a cloning/imaging/rescue suite/inventory management system	Command Injection	Prior to 1.5.10.34	1.5.10.34	https://fogproject.org/ https://github.com/FOGProject/fogproject/security/advisories/GHSA-7h44-6vq6-cq8j
https://nvd.nist.gov/vuln/detail/CVE-2024-28074	9.6	SolarWinds Access Rights Manager	Deserialization of Untrusted Data	N/A	N/A	https://www.solarwinds.com/access-rights-manager https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2024-3_release_notes.htm
https://nvd.nist.gov/vuln/detail/CVE-2024-6834	9	APIML Spring Cloud Gateway	privilege escalation	N/A	N/A	https://docs.zowe.org/v2.12.x/user-guide/api-mediation/api-mediation-internal-configuration/ https://github.com/zowe/api-layer
https://nvd.nist.gov/vuln/detail/CVE-2024-20435	8.8	Cisco AsyncOS for Secure Web Appliance	Execution with Unnecessary	N/A	N/A	https://www.cisco.com/c/en/us/support/security/web-security-appliance/series.html https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-swa-priv-esc-

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
			Privileges			7uHpZsCC
https://nvd.nist.gov/vuln/detail/CVE-2024-5471	8.8	Zohocorp ManageEngine DDI Central	Use of Hard-coded Credentials	4001	N/A	https://store.manageengine.com/dns-dhcp-ipam/ https://www.manageengine.com/dns-dhcp-ipam/security-updates/cve-2024-5471.html
https://nvd.nist.gov/vuln/detail/CVE-2023-46801	8.8	Apache Linkis DataSource	Deserialization of Untrusted Data	<= 1.5.0	N/A	https://linkis.apache.org/docs/1.1.1/deployment/start-metadatasource/ https://lists.apache.org/thread/0dnzh64xy1n7qo3rgo2loz9zn7m9xgdx
https://nvd.nist.gov/vuln/detail/CVE-2024-5325	8.8	Form Vibes plugin for WordPress	SQL Injection	all versions up to, and including, 1.4.10	N/A	https://wordpress.org/plugins/form-vibes/ https://www.wordfence.com/threat-intel/vulnerabilities/id/a3311097-d477-441e-9bf3-3f991a9b6af9?source=cve
https://nvd.nist.gov/vuln/detail/CVE-2024-21136	8.6	Oracle Retail Xstore Office	compromise of service	19.0.5, 20.0.3, 20.0.4, 22.0.0 and	N/A	https://docs.oracle.com/cd/E62107_01/xoffice/index.html https://www.oracle.com/security-alerts/cpujul2024.html

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
				23.0.1		
https://nvd.nist.gov/vuln/detail/CVE-2024-21141	8.2	Oracle VM VirtualBox	compromise of service	Prior to 7.0.20	N/A	https://www.virtualbox.org/ https://www.oracle.com/security-alerts/cpujul2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-21152	8.1	Oracle Process Manufacturing Financials	vulnerability can result in unauthorized creation, deletion or modification access to critical data	12.2.12-12.2.13	N/A	https://docs.oracle.com/cd/A60725_05/pdf/gemmsfi.pdf https://www.oracle.com/security-alerts/cpujul2024.html
https://nvd.nist.gov/vuln/detail/CVE-2024-21146	8.1	Oracle Trade Management	compromise of service	12.2.3-12.2.13	N/A	https://docs.oracle.com/cd/E18727_01/doc.121/e13590/T327028T446903.htm https://www.oracle.com/security-alerts/cpujul2024.html

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-32861	7.8	Software House C?CURE 9000 Site Server	Incorrect Default Permissions	N/A	N/A	https://www.swhouse.com/products/software_CCU_RE9000_siteserver https://www.cisa.gov/news-events/ics-advisories/ICSA-24-191-05 https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories
https://nvd.nist.gov/vuln/detail/CVE-2022-45449	7.7	Acronis Cyber Protect 15	Exposure of Sensitive Information to an Unauthorized Actor	before build 30984	N/A	https://www.acronis.com/en-us/support/protect/15/ https://security-advisory.acronis.com/advisories/SEC-5279
https://nvd.nist.gov/vuln/detail/CVE-2024-3232	7.6	Tenable Identity Exposure	Improper Neutralization of Formula Elements in a CSV File	N/A	N/A	https://www.tenable.com/products/identity-exposure https://www.tenable.com/security/tns-2024-04

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
https://nvd.nist.gov/vuln/detail/CVE-2024-20323	7.5	Cisco Intelligent Node	Use of Hard-coded Cryptographic Key	N/A	N/A	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-inode-static-key-VUVCeynn https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-inode-static-key-VUVCeynn
https://nvd.nist.gov/vuln/detail/CVE-2024-21147	7.4	Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot)	compromise of service	Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1;	N/A	https://www.oracle.com/security-alerts/cpujul2024.html

CVEs						
URL ευπάθειας (NIST NVD)	CVSSv3	Προϊόν/Υπηρεσία	Τύπος Ευπάθειας	Συσκευές/ Εκδόσεις που επηρεάζονται	Συσκευές/ Εκδόσεις που ΔΕΝ επηρεάζονται	URL προϊόντος/υπηρεσίας URL οδηγιών αντιμετώπισης
				Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10		
https://nvd.nist.gov/vuln/detail/CVE-2024-39917	7.2	xrdp is an open source RDP server	Improper Restriction of Excessive Authentication Attempts	prior to 0.10.0	N/A	https://www.xrdp.org/ https://github.com/neutrino-labs/xrdp/security/advisories/GHSA-7w22-h4w7-8j5j

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας	URL
CISA Releases Industrial Control Systems Advisories	<p>ICSA-24-200-01 Mitsubishi Electric MELSOFT MaiLab</p> <p>ICSA-24-200-02 Subnet Solutions PowerSYSTEM Center</p> <p>ICSMA-24-200-01 Philips Vue PACS</p> <p>ICSA-24-193-01 Siemens Remote Connect Server</p> <p>ICSA-24-193-02 Siemens RUGGEDCOM APE 1808</p> <p>ICSA-24-193-03 Siemens Teamcenter Visualization and JT2Go</p> <p>ICSA-24-193-04 Siemens Simcenter Femap</p> <p>ICSA-24-193-05 Siemens SCALANCE, RUGGEDCOM, SIPLUS, and SINEC</p> <p>ICSA-24-193-06 Siemens RUGGEDCOM</p> <p>ICSA-24-193-07 Siemens SIMATIC and SIMIT</p> <p>ICSA-24-193-08 Siemens Mendix Encryption Module</p> <p>ICSA-24-193-09 Siemens SINEMA Remote Connect Server</p> <p>ICSA-24-193-10 Siemens JT Open and PLM XML SDK</p> <p>ICSA-24-193-11 Siemens RUGGEDCOM APE 1808</p> <p>ICSA-24-193-12 Siemens TIA Portal and SIMATIC STEP 7</p> <p>ICSA-24-193-13 Siemens TIA Portal, SIMATIC, and SIRIUS</p> <p>ICSA-24-193-14 Siemens SIPROTEC</p>	<p>https://www.cisa.gov/news-events/alerts/2024/07/18/cisa-releases-three-industrial-control-systems-advisories</p> <p>https://www.cisa.gov/news-events/alerts/2024/07/11/cisa-releases-twenty-one-industrial-control-systems-advisories</p>

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας	URL
	<p>ICSA-24-193-15 Siemens SINEMA Remote Connect Server</p> <p>ICSA-24-193-16 Siemens SIMATIC WinCC</p> <p>ICSA-24-193-17 Siemens SIMATIC STEP 7 (TIA Portal)</p> <p>ICSA-24-193-18 Rockwell Automation ThinManager ThinServer</p> <p>ICSA-24-193-19 Rockwell Automation FactoryTalk System Services and Policy Manager</p> <p>ICSA-24-193-20 HMS Industrial Networks Anybus-CompactCom 30</p> <p>ICSA-22-356-03 Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series (Update D)</p>	

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας	URL
Cisco Releases Security Updates for Multiple Products	Cisco Secure Email Gateway Arbitrary File Write Vulnerability Cisco Smart Software Manager On-Prem Password Change Vulnerability Cisco Secure Web Appliance Privilege Escalation Vulnerability Cisco Identity Services Engine Arbitrary File Upload Vulnerability Cisco Intelligent Node Software Static Key Vulnerability Cisco Webex App Vulnerabilities Cisco RV340 and RV345 Dual WAN Gigabit VPN Routers Authenticated Remote Code Execution Vulnerability Cisco Expressway Series Open Redirect Vulnerability Cisco Secure Email Gateway Server-Side Template Injection Vulnerability	https://www.cisa.gov/news-events/alerts/2024/07/18/cisco-releases-security-updates-multiple-products
Ivanti Releases Security Updates for Endpoint Manager	Security Advisory EPM Security Advisory Ivanti Endpoint Manager for Mobile (EPMM)	https://www.cisa.gov/news-events/alerts/2024/07/18/ivanti-releases-security-updates-endpoint-manager
Oracle Releases Critical Patch Update Advisory for July 2024	July 2024 Critical Patch Update Advisory	https://www.cisa.gov/news-events/alerts/2024/07/18/oracle-releases-critical-patch-update-advisory-july-2024
CISA Adds Three Known Exploited Vulnerabilities to Catalog	CVE-2024-34102 Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability CVE-2024-28995 SolarWinds Serv-U Path Traversal	https://www.cisa.gov/news-events/alerts/2024/07/17/cisa-adds-three-known-exploited-vulnerabilities-catalog

CISA/CERT-EU Alerts & Advisories		
Σύντομη περιγραφή / Τίτλος	Αναγνωριστικό ευπάθειας	URL
	Vulnerability CVE-2022-22948 VMware vCenter Server Incorrect Default File Permissions Vulnerability	
Microsoft Releases July 2024 Security Updates	Microsoft Security Update Guide for July	https://www.cisa.gov/news-events/alerts/2024/07/09/microsoft-releases-july-2024-security-updates
Adobe Releases Security Updates for Multiple Products	Security Updates Available for Adobe Premiere Pro APSB24-46 Security Update Available for Adobe InDesign APSB24-48 Security Updates Available for Adobe Bridge APSB24-51	https://www.cisa.gov/news-events/alerts/2024/07/09/adobe-releases-security-updates-multiple-products