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-2019-20467	**9.8**	Sannce Smart HD Wifi Security Camera EAN 2 Το συγκεκριμένο αναφέρεται σε πολλές συσκευές με παλιές ευπάθειες	TELNET interface available by default	950004 595317	N/A	https://www.sannce.com/ http://seclists.org/fulldisclosure/2024/Jul/14
https://nvd.nist.gov/vuln/detail/CVE-2024-6748	**8.3**	Zohocorp ManageEngine OpManager, OpManager Plus, OpManager MSP and RMM	SQL Injection	versions 128317 and below	N/A	https://www.manageengine.com/about-us.html https://www.manageengine.com/itom/advisory/cve-2024-6748.html
https://nvd.nist.gov/vuln/detail/CVE-	**7.8**	Comodo Internet	Local Privilege	N/A	N/A	https://www.comodo.com/home/internet-security/internet-security-pro.php

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
2024-7248		Security Pro	Escalation			https://www.zerodayinitiative.com/advisories/ZDI-24-953/
https://nvd.nist.gov/vuln/detail/CVE-2024-7249	**7.8**	Comodo Firewall	Local Privilege Escalation	N/A	N/A	https://personalfirewall.comodo.com/ https://www.zerodayinitiative.com/advisories/ZDI-24-954/
https://nvd.nist.gov/vuln/detail/CVE-2024-6387	**8.1**	OpenSSH's server (sshd)	race condition	N/A	N/A	https://www.openssh.com/ **Please check the full list here for security advisories that apply to your needs.** https://nvd.nist.gov/vuln/detail/CVE-2024-6387
https://nvd.nist.gov/vuln/detail/CVE-2024-7213	**8.8**	TOTOLINK A7000R	buffer overflow	9.1.0u.6268_B20220504	N/A	https://www.totolink.net/home/menu/newstpl/menu_newstpl/products/id/171.html https://github.com/abcdefg-png/IoT-vulnerable/blob/main/TOTOLINK/A7000R/setWizardCfg.md
https://nvd.nist.gov/vuln/detail/CVE-2024-4558	**7.5**	Google Chrome	Use after free	prior to 124.0.6367.155	N/A	https://www.google.com/chrome/ http://seclists.org/fulldisclosure/2024/Jul/18

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-2024-27316	**7.5**	Http server (apache)	memory exhaustion	N/A	N/A	https://httpd.apache.org/ https://httpd.apache.org/security/vulnerabilities_24.html
https://nvd.nist.gov/vuln/detail/CVE-2024-27804	**8.1**	Apple OS	execute arbitrary code with kernel privileges	N/A	iOS 17.5 and iPadOS 17.5, tvOS 17.5, watchOS 10.5, macOS Sonoma 14.5	https://support.apple.com https://support.apple.com/en-us/HT214101 https://support.apple.com/en-us/HT214102 https://support.apple.com/en-us/HT214104 https://support.apple.com/en-us/HT214106 https://support.apple.com/kb/HT214101 https://support.apple.com/kb/HT214102 https://support.apple.com/kb/HT214104 https://support.apple.com/kb/HT214106 https://support.apple.com/kb/HT214123

CISA/CERT-EU Alerts & Advisories

Σύντομη περιγραφή / Τίτλος	**Αναγνωριστικό ευπάθειας**	**URL**
CISA Adds Known Exploited Vulnerabilities to Catalog	CVE-2024-4879 ServiceNow Improper Input Validation Vulnerability CVE-2024-5217 ServiceNow Incomplete List of Disallowed Inputs Vulnerability CVE-2023-45249 Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability CVE-2024-37085 VMware ESXi Authentication Bypass Vulnerability	https://www.cisa.gov/news-events/alerts/2024/07/29/cisa-adds-three-known-exploited-vulnerabilities-catalog https://www.cisa.gov/news-events/alerts/2024/07/30/cisa-adds-one-known-exploited-vulnerability-catalog
Apple Releases Security Updates for Multiple Products	Safari 17.6, iOS 17.6 and iPadOS 17.6, iOS 16.7.9 and iPadOS 16.7.9, macOS Sonoma 14.6, macOS Ventura 13.6.8, macOS Monterey 12.7.6, watchOS 10.6, tvOS 17.6, visionOS 1.3	https://www.cisa.gov/news-events/alerts/2024/07/30/apple-releases-security-updates-multiple-products