Cyber WAR - Threat Intelligence & OSINT Publication

Threat Intelligence and OSINT Publication

April 6, 2026

==========

Date and Summary

April 6, 2026

Summary
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets is a community revolving around all layers of cybersecurity. There are now multiple media types being produced. We have out video series and the printed media.

Video Access:

* Amazon FireTV App - amzn.to/30oiUpE (https://amzn.to/30oiUpE)

* YouTube - youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg (https://www.youtube.com/channel/UCVjF2YkyJ8C9HUIGgdMXybg)

Printed / Kindle Publications:

* Cyber Secrets on Amazon - amzn.to/2UuIG9B (https://amzn.to/2UuIG9B)

Capture the Flag (CTF) Events:

* Avengers Arsenal CTF - Ends November 15th (https://informationwarfarecenter.com/files/CTF%20-%20Avengers%20Arsenal%20Challenge.pdf)

* Reverse Engineering CTF - Ends November 15th (https://informationwarfarecenter.com/files/CTF%20-%20RE_CSI_Forensic_Challenge_2020q2.pdf)

Interesting News

Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.

https://training.csilinux.com/course/view.php?id=5 (https://training.csilinux.com/course/view.php?id=5)

Packet Storm Security

Krebs on Security

---

* Germany Doxes UNKN, Head of RU Ransomware Gangs REvil, GandCrab - https://krebsonsecurity.com/2026/04/germany-doxes-unkn-head-of-ru-ransomware-gangs-revil-gandcrab/
* CanisterWorm Springs Wiper Attack Targeting Iran - https://krebsonsecurity.com/2026/03/canisterworm-springs-wiper-attack-targeting-iran/
* Feds Disrupt IoT Botnets Behind Huge DDoS Attacks - https://krebsonsecurity.com/2026/03/feds-disrupt-iot-botnets-behind-huge-ddos-attacks/
* Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker - https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/
* Microsoft Patch Tuesday, March 2026 Edition - https://krebsonsecurity.com/2026/03/microsoft-patch-tuesday-march-2026-edition/
* How AI Assistants are Moving the Security Goalposts - https://krebsonsecurity.com/2026/03/how-ai-assistants-are-moving-the-security-goalposts/
* Who is the Kimwolf Botmaster Dort ? - https://krebsonsecurity.com/2026/02/who-is-the-kimwolf-botmaster-dort/
* Starkiller Phishing Service Proxies Real Login Pages, MFA - https://krebsonsecurity.com/2026/02/starkiller-phishing-service-proxies-real-login-pages-mfa/
* Kimwolf Botnet Swamps Anonymity Network I2P - https://krebsonsecurity.com/2026/02/kimwolf-botnet-swamps-anonymity-network-i2p/
* Patch Tuesday, February 2026 Edition - https://krebsonsecurity.com/2026/02/patch-tuesday-february-2026-edition/

Dark Reading

The Hacker News

---

* Iran-Linked Password-Spraying Campaign Targets 300+ Israeli Microsoft 365 Organizations - https://thehackernews.com/2026/04/iran-linked-password-spraying-campaign.html
* DPRK-Linked Hackers Use GitHub as C2 in Multi-Stage Attacks Targeting South Korea - https://thehackernews.com/2026/04/dprk-linked-hackers-use-github-as-c2-in.html
* Multi-OS Cyberattacks: How SOCs Close a Critical Risk in 3 Steps - https://thehackernews.com/2026/04/multi-os-cyberattacks-how-socs-close.html
* ? Weekly Recap: Axios Hack, Chrome 0-Day, Fortinet Exploits, Paragon Spyware and More - https://thehackernews.com/2026/04/weekly-recap-axios-hack-chrome-0-day.html
* How LiteLLM Turned Developer Machines Into Credential Vaults for Attackers - https://thehackernews.com/2026/04/how-litellm-turned-developer-machines.html
* Qilin and Warlock Ransomware Use Vulnerable Drivers to Disable 300+ EDR Tools - https://thehackernews.com/2026/04/qilin-and-warlock-ransomware-use.html
* BKA Identifies REvil Leaders Behind 130 German Ransomware Attacks - https://thehackernews.com/2026/04/bka-identifies-revil-leaders-behind-130.html
* $285 Million Drift Hack Traced to Six-Month DPRK Social Engineering Operation - https://thehackernews.com/2026/04/285-million-drift-hack-traced-to-six.html
* 36 Malicious npm Packages Exploited Redis, PostgreSQL to Deploy Persistent Implants - https://thehackernews.com/2026/04/36-malicious-npm-packages-exploited.html
* Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS - https://thehackernews.com/2026/04/fortinet-patches-actively-exploited-cve.html

* China-Linked TA416 Targets European Governments with PlugX and OAuth-Based Phishing - https://thehackernews.com/2026/04/china-linked-ta416-targets-european.html
* Microsoft Details Cookie-Controlled PHP Web Shells Persisting via Cron on Linux Servers - https://thehackernews.com/2026/04/microsoft-details-cookie-controlled-php.html
* UNC1069 Social Engineering of Axios Maintainer Led to npm Supply Chain Attack - https://thehackernews.com/2026/04/unc1069-social-engineering-of-axios.html
* Why Third-Party Risk Is the Biggest Gap in Your Clients' Security Posture - https://thehackernews.com/2026/04/why-third-party-risk-is-biggest-gap-in.html
* New SparkCat Variant in iOS, Android Apps Steals Crypto Wallet Recovery Phrase Images - https://thehackernews.com/2026/04/new-sparkcat-variant-in-ios-android.html

---

Security Week

---

* Google DeepMind Researchers Map Web Attacks Against AI Agents - https://www.securityweek.com/google-deepmind-researchers-map-web-attacks-against-ai-agents/
* Guardarian Users Targeted With Malicious Strapi NPM Packages - https://www.securityweek.com/guardarian-users-targeted-with-malicious-strapi-npm-packages/
* North Korean Hackers Target High-Profile Node.js Maintainers - https://www.securityweek.com/north-korean-hackers-target-high-profile-node-js-maintainers/
* Fortinet Rushes Emergency Fixes for Exploited Zero-Day - https://www.securityweek.com/fortinet-rushes-emergency-fixes-for-exploited-zero-day/
* European Commission Confirms Data Breach Linked to Trivy Supply Chain Attack - https://www.securityweek.com/european-commission-confirms-data-breach-linked-to-trivy-supply-chain-attack/
* TrueConf Zero-Day Exploited in Asian Government Attacks - https://www.securityweek.com/trueconf-zero-day-exploited-in-asian-government-attacks/
* In Other News: ChatGPT Data Leak, Android Rootkit, Water Facility Hit by Ransomware - https://www.securityweek.com/in-other-news-chatgpt-data-leak-android-rootkit-water-facility-hit-by-ransomware/
* Critical ShareFile Flaws Lead to Unauthenticated RCE - https://www.securityweek.com/critical-sharefile-flaws-lead-to-unauthenticated-rce/
* Mobile Attack Surface Expands as Enterprises Lose Control - https://www.securityweek.com/mobile-attack-surface-expands-as-enterprises-lose-control/
* React2Shell Exploited in Large-Scale Credential Harvesting Campaign - https://www.securityweek.com/react2shell-exploited-in-large-scale-credential-harvesting-campaign/

KnowBe4 Security Awareness Training Blog

---

* Your KnowBe4 Fresh Compliance Plus Content Updates | March 2026 - https://blog.knowbe4.com/your-knowbe4-fresh-compliance-plus-content-updates-march-2026
* Detection and Prevention of Misdirected Emails: What to Know - https://blog.knowbe4.com/detection-and-prevention-of-misdirected-emails-what-to-know
* Outbound Email Security: Protecting Data and Reputation - https://blog.knowbe4.com/outbound-email-security-protecting-data-and-reputation-1
* Your KnowBe4 Fresh Content Updates from March 2026 - https://blog.knowbe4.com/your-knowbe4-fresh-content-updates-from-march-2026
* Phishing Attacks Are Exploiting the War in Iran - https://blog.knowbe4.com/phishing-attacks-exploiting-iran-war
* How to Prevent Phishing Emails by Reducing Human Risk - https://blog.knowbe4.com/how-to-prevent-phishing-emails-by-reducing-human-risk
* Chronic Resource Constraints: Doing More With Less in Public Sector Cybersecurity - https://blog.knowbe4.com/chronic-resource-constraints-doing-more-with-less-in-public-sector-cybersecurity
* Unrelenting Threats Against Government and Education: Why Human Risk Is the Front Line - https://blog.knowbe4.com/unrelenting-threats-against-government-and-education-why-human-risk-is-the-front-line
* CyberheistNews Vol 16 #13 The 'Urgency Trap': Why Time Pressure is Your Biggest Email Red Flag -

https://blog.knowbe4.com/cyberheistnews-vol-16-13-the-urgency-trap-why-time-pressure-is-your-biggest-email-red-flag
* World Backup Day: Because It Won t Happen to Me Often Means It Will - https://blog.knowbe4.com/world-backup-day-because-it-wont-happen-to-me-often-means-it-will

---

HackRead

---

* Missile Alert Phishing Exploits Iran-US-Israel Conflict for Microsoft Logins - https://hackread.com/missile-alert-phishing-iran-us-israel-microsoft-logins/
* Cloudflare Targets WordPress With New AI-Powered EmDash CMS - https://hackread.com/cloudflare-wordpress-ai-powered-emdash-cms/
* Why Security Researchers and Red Teams Are Turning to Workflow Automation - https://hackread.com/security-researchers-red-teams-workflow-automation/
* North Korean Hackers Pose as Trading Firm to Steal $285M from Drift - https://hackread.com/north-korean-hackers-trading-firm-drift-protocol/
* BrowserGate: LinkedIn Tracks 6,000+ Browser Extensions on Users PCs - https://hackread.com/browsergate-linkedin-track-browser-extensions-user-pc/
* UNC1069 Targets Node.js Maintainers via Fake LinkedIn, Slack Profiles - https://hackread.com/unc1069-node-js-maintainer-fake-linkedin-slack-profile/
* Fake ChatGPT Ad Blocker Chrome Extension Caught Spying on Users - https://hackread.com/fake-chatgpt-ad-blocker-chrome-extension-spy-users/

Advisories

---

* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/04/06/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/04/02/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/04/01/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/03/30/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/03/27/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/03/26/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds One Known Exploited Vulnerability to Catalog - https://www.cisa.gov/news-events/alerts/2026/03/25/cisa-adds-one-known-exploited-vulnerability-catalog
* CISA Adds Five Known Exploited Vulnerabilities to Catalog - https://www.cisa.gov/news-events/alerts/2026/03/20/cisa-adds-five-known-exploited-vulnerabilities-catalog

* Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a
* CISA Shares Lessons Learned from an Incident Response Engagement - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-266a

* Vulnerability Summary for the Week of February 2, 2026 - https://www.cisa.gov/news-events/bulletins/sb26-040
* Vulnerability Summary for the Week of January 26, 2026 - https://www.cisa.gov/news-events/bulletins/sb26-033

ZDI-CAN-29653: Adobe - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'DongHyeon Hwang (kind_killerwhale)' was reported to the

affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30003: Microsoft - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'mad31k' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29388: Avast - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'aviel zohar' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29483: Apple - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of TrendAI Zero Day Initiative' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30002: TrendAI - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lays (@_L4ys) of TRAPA Security' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30288: Samsung - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of TrendAI Zero Day Initiative' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30179: TrendAI - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lays (@_L4ys) of TRAPA Security' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30052: Microsoft - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.0 AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'mad31k' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30180: TrendAI - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lays (@_L4ys) of TRAPA Security' was reported to the affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-30215: TrendAI - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'Lays (@_L4ys) of TRAPA Security' was reported to the
affected vendor on: 2026-04-01, 5 days ago. The vendor is given until 2026-07-30 to publish a
fix or workaround. Once the vendor has created and tested a patch we will coordinate the release
of a public advisory.
ZDI-CAN-30346: BlackBerry - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'Mat Powell of TrendAI Zero Day Initiative' was reported to
the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish
a fix or workaround. Once the vendor has created and tested a patch we will coordinate the
release of a public advisory.
ZDI-CAN-28149: Bosch Rexroth - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'kimiya' was reported to the affected vendor on:
2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround.
Once the vendor has created and tested a patch we will coordinate the release of a public
advisory.
ZDI-CAN-29337: OriginLab - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2026-03-31,
6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor
has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29536: pdfforge - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'Natnael Samson (@NattiSamson)' was reported to the
affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a
fix or workaround. Once the vendor has created and tested a patch we will coordinate the release
of a public advisory.
ZDI-CAN-29336: OriginLab - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2026-03-31,
6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor
has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29120: GNU - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 5.9 AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
severity vulnerability discovered by 'PeikaiLi' was reported to the affected vendor on:
2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround.
Once the vendor has created and tested a patch we will coordinate the release of a public
advisory.
ZDI-CAN-30175: Microsoft - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 5.8 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N)
severity vulnerability discovered by 'Nelson William Gamazo Sanchez of TrendAI Research' was
reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29
to publish a fix or workaround. Once the vendor has created and tested a patch we will
coordinate the release of a public advisory.
ZDI-CAN-29370: Oracle - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
(https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
severity vulnerability discovered by 'Dvir Gozlan' was reported to the affected vendor on:
2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround.

Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-28898: GIMP - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30176: Microsoft - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 5.8 AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N) severity vulnerability discovered by 'Nelson William Gamazo Sanchez of TrendAI Research' was reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-28718: TrendAI - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 5.6 AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Zeze and Sharkkcode with TeamT5' was reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29496: dnsmasq - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xander Mackenzie | @thetrueartist' was reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-30243: Google - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 6.5 AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H) severity vulnerability discovered by 'Nitesh Surana (niteshsurana.com) of TrendAI Research' was reported to the affected vendor on: 2026-03-31, 6 days ago. The vendor is given until 2026-07-29 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-29790: Linux - http://www.zerodayinitiative.com/advisories/upcoming/
A CVSS score 8.5 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H (https://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'DongHyeon Hwang (kind_killerwhale)' was reported to the affected vendor on: 2026-03-30, 7 days ago. The vendor is given until 2026-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Exploits

---

* [local] is-localhost-ip 2.0.0 - SSRF - https://www.exploit-db.com/exploits/52496
* [webapps] Fortinet FortiWeb v8.0.1 - Auth Bypass - https://www.exploit-db.com/exploits/52495
* [local] Windows Kernel - Elevation of Privilege - https://www.exploit-db.com/exploits/52494
* [local] Desktop Window Manager Core Library 10.0.10240.0 - Privilege Escalation - https://www.exploit-db.com/exploits/52493
* [webapps] ASP.net 8.0.10 - Bypass - https://www.exploit-db.com/exploits/52492
* [webapps] Grafana 11.6.0 - SSRF - https://www.exploit-db.com/exploits/52491
* [webapps] Zhiyuan OA - arbitrary file upload leading - https://www.exploit-db.com/exploits/52490

* [webapps] WBCE CMS 1.6.4 - Remote Code Execution - https://www.exploit-db.com/exploits/52489
* [webapps] RiteCMS 3.1.0 - Authenticated Remote Code Execution - https://www.exploit-db.com/exploits/52488
* [webapps] WordPress Madara - Local File Inclusion - https://www.exploit-db.com/exploits/52487
* [webapps] WordPress Backup Migration 1.3.7 - Remote Command Execution - https://www.exploit-db.com/exploits/52486
* [webapps] mailcow 2025-01a - Host Header Password Reset Poisoning - https://www.exploit-db.com/exploits/52485
* [webapps] Easy File Sharing Web Server v7.2 - Buffer Overflow - https://www.exploit-db.com/exploits/52484
* [webapps] WeGIA 3.5.0 - SQL Injection - https://www.exploit-db.com/exploits/52483
* [webapps] Boss Mini v1.4.0 - Local File Inclusion (LFI) - https://www.exploit-db.com/exploits/52482
* [webapps] motionEye 0.43.1b4 - RCE - https://www.exploit-db.com/exploits/52481
* [remote] Windows 10.0.17763.7009 - spoofing vulnerability - https://www.exploit-db.com/exploits/52480
* [local] glibc 2.38 - Buffer Overflow - https://www.exploit-db.com/exploits/52479
* [remote] windows 10/11 - NTLM Hash Disclosure Spoofing - https://www.exploit-db.com/exploits/52478
* [remote] Redis 8.0.2 - RCE - https://www.exploit-db.com/exploits/52477
* [webapps] OctoPrint 1.11.2 - File Upload - https://www.exploit-db.com/exploits/52476
* [remote] Ingress-NGINX Admission Controller v1.11.1 - FD Injection to RCE - https://www.exploit-db.com/exploits/52475
* [webapps] aiohttp 3.9.1 - directory traversal PoC - https://www.exploit-db.com/exploits/52474
* [webapps] FortiWeb Fabric Connector 7.6.x - SQL Injection to Remote Code Execution - https://www.exploit-db.com/exploits/52473
* [local] Docker Desktop 4.44.3 - Unauthenticated API Exposure - https://www.exploit-db.com/exploits/52472

* Kanboard < = 1.2.50 Authenticated SQL Injection - https://cxsecurity.com/issue/WLB-2026030027
* OpenClaw tools.exec.safeBins < = 2026.2.22 Remote Code Execution - https://cxsecurity.com/issue/WLB-2026030004
* Google Chrome < 145.0.7632.75 - CSSFontFeatureValuesMap Use-After-Free - https://cxsecurity.com/issue/WLB-2026020022
* Siklu EtherHaul Series EH-8010 Remote Command Execution - https://cxsecurity.com/issue/WLB-2026020013
* aiohttp 3.9.1 Directory Traversal - https://cxsecurity.com/issue/WLB-2026020007
* deephas < = 1.0.7 - Prototype Pollution leading to Arbitrary Code Execution / DoS - https://cxsecurity.com/issue/WLB-2026020005
* LangChain Core - Serialization Injection to Jinja2 SSTI/RCE - https://cxsecurity.com/issue/WLB-2026010017

Dark Web News
