DFN-CERT

deutsches forschungsnetz

Neues aus dem DFN-CERT

85. Betriebstagung | 06.10.2026

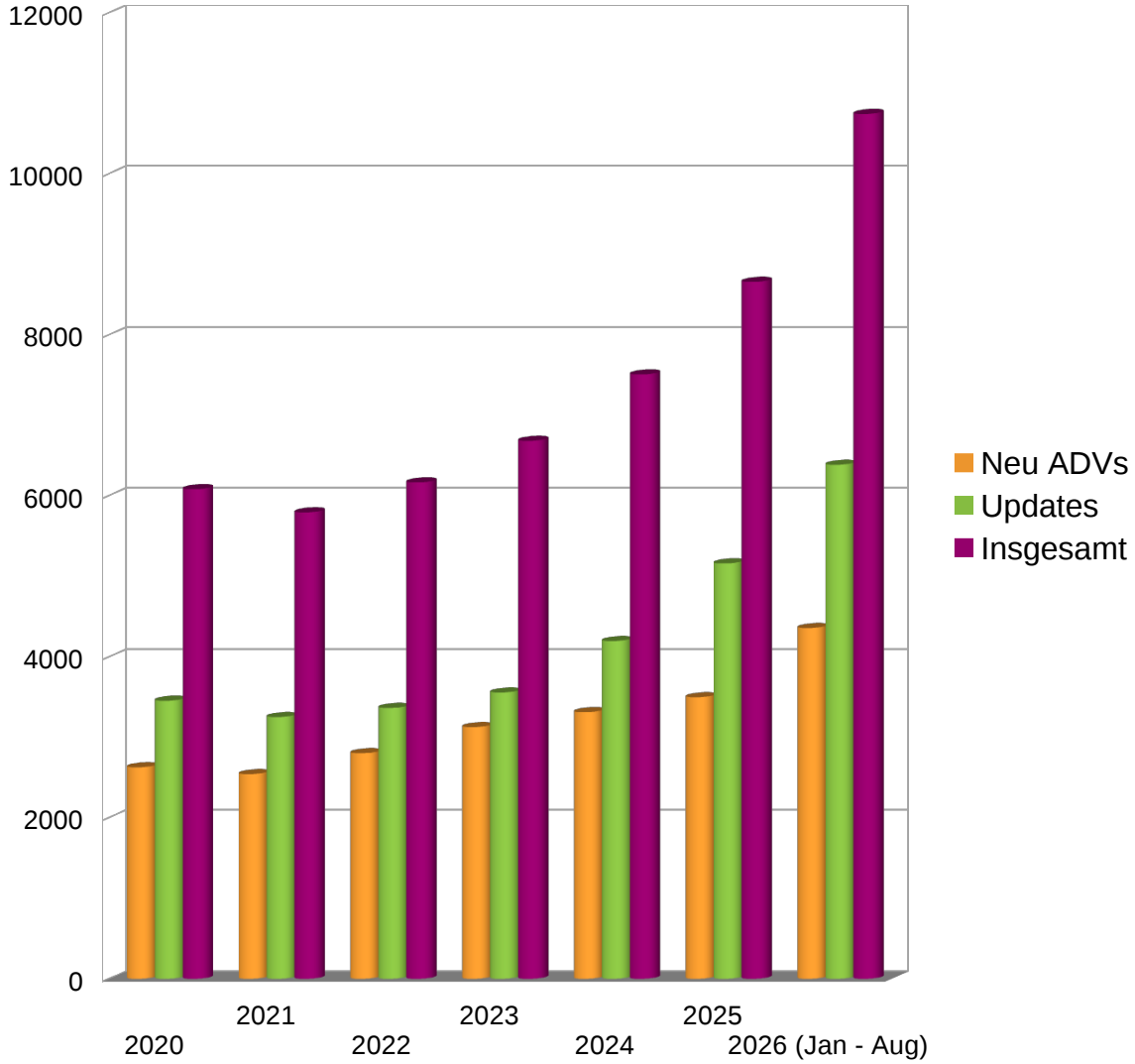
Christine Kahl

Agenda

1. Schwachstellenmeldungen
2. AW-Meldungen
3. Ankündigungen

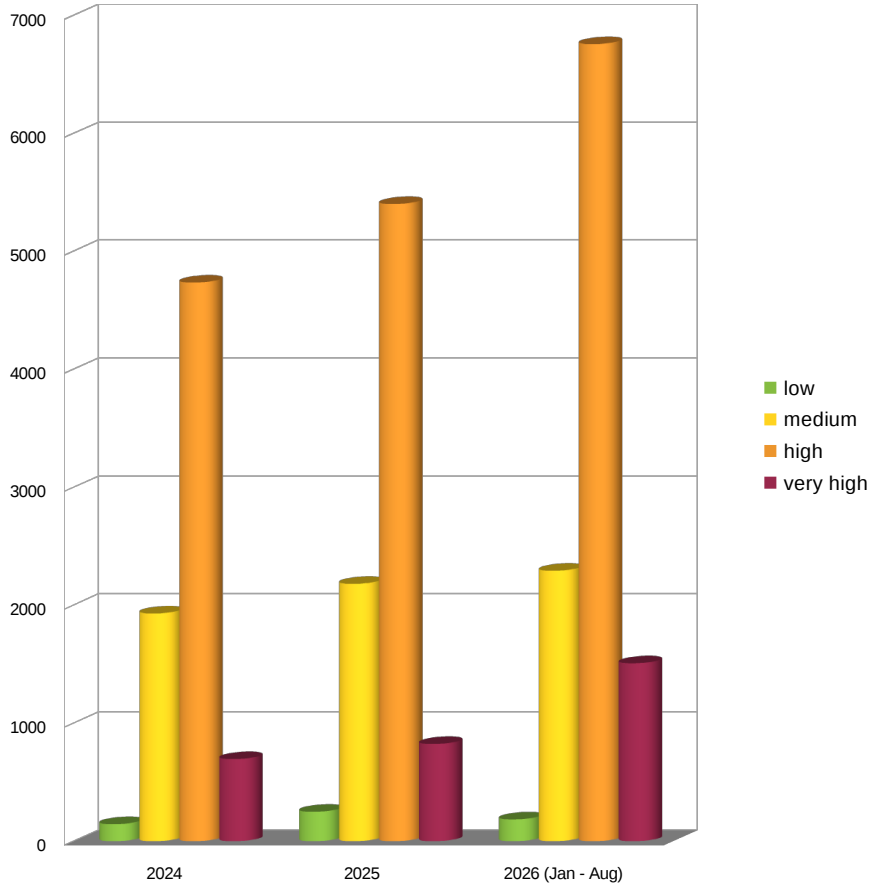
Schwachstellenmeldungen

Aktuelle Advisory Zahlen



- Gesamtzahlen
  - 2025: 8.659
  - 2024: 7.509
  - 2026 ersten drei Quartale: 10.744
  - Ohne Vereinfachungen beim Erstellen der Meldungen nicht zu machen
- Prognose 2026
  - Mehr als 15.000 Meldungen

ADVs nach CVSS Schweregrad – 2024 - 2026



- Very High überproportional gestiegen.
- Ist es schlimm? Ja, schon, aber ...
- High Meldungen
  - 2024 = 4736, ca. 395 pro Monat
  - 2025 = 5402, ca. 450 pro Monat
  - Jan - Aug 26 = 6757, ca. 750 pro Monat
- Very high Meldungen
  - 2024 = 697, ca. 58 pro Monat
  - 2025 = 825, ca. 68 pro Monat
  - Jan - Aug 26 = 1509, ca. 167 pro Monat, aber nicht wirklich gleich verteilt, Juli und Aug über 300

Geänderte Schwachstellenmeldungen – Warum?

- Die Anzahl der Schwachstellenmeldungen steigt seit Jahren kontinuierlich, hat jetzt aber, nicht zuletzt durch den Einsatz von KI zum Finden von Schwachstellen, einen deutlichen Schub erfahren.
- Neben einer höheren Frequenz der Patch-Veröffentlichungen, steigt auch die Zahl der behobenen Schwachstellen.
- Bsp. hat Chrome in den ersten 5,5 Monaten 2026 die zehnfache Menge an Schwachstellen behoben, wie im gleichen Zeitraum in 2025.
- Jede dieser Schwachstellen einzeln zu analysieren und zu beschreiben, nimmt viel Zeit in Anspruch und verzögert dadurch die Bereitstellung der Information.
- Wir glauben (hoffen), dass es Ihnen mehr hilft, wenn wir uns auf die wichtigsten Schwachstellen fokussieren und versuchen die Informationen möglichst schnell zu verteilen.

Geänderte Schwachstellenmeldungen – Wie?

- Seit dem 06. Juli 26 werden bei Schwachstellenmeldungen, die mehr als fünf Schwachstellen adressieren, eventuell nicht mehr alle einzeln analysiert und beschrieben, sondern der Fokus wird auf die schwerwiegendsten gelegt.
- Bei Herstellern wie Android, Google (Chrome), F5, HP, Juniper, Mozilla und Mircrosoft selektieren wir die schwerwiegendsten Schwachstellen auf Basis der mitgelieferten Einstufung.
- Liefert der Hersteller diese Einstufung nicht, wie z. B. bei Oracle, erfolgt die Selektion auf Basis des CVSS.
- Und stellt der Hersteller auch keinen Score bereit, selektieren die Kollegen auf Basis ihrer Erfahrung.
- Kritische Schwachstellen im einstelligen Bereich werden einzeln betrachtet und bei größerer Anzahl in einer Meldung ebenfalls selektiert bzw. zusammengefasst.
- Dieses Vorgehen setzen wir analog für Sicherheitsupdates für Unix/Linux- Distributionen um.

Geänderte Schwachstellenmeldungen – Wie?

- Wenn wir Schwachstellen aus der Einzelbetrachtung herausfallen lassen, dann machen wir das in der Meldung kenntlich.
- Wenn Referenzen zu den einzelnen Schwachstellen verfügbar sind, wie u. a. auch NVD, dann werden diese weiterhin in die Meldung aufgenommen.
- Unser Vorgehen reduziert also den Umfang der erzeugten Meldungen, es fallen aber keine weg.

Nächste Frage: **Bleibt das so?**

Ehrliche Antwort: **Hoffentlich!**

Kritische Schwachstellen mit CVSS ab 9.8

(ausgewählt seit der letzten BT im März 2026)

- Cisco Firewall (CVE-2026-20131, 10.0; CVE-2026-20079, 10.0; CVE-2026-20002, 8.2): Schwachstellen ermöglichen das Ausführen beliebigen Programmcodes, Umgehen von Sicherheitsvorkehrungen und SQL-Injection. CVE-2026-20131 wurde zügig nach Veröffentlichung ausgenutzt.

- FreeBSD (CVE- ….

- Oder doch anders:
  - Entsprechend der gestiegenen Meldungszahlen ist die List der besonders beachtenswerten Schwachstellen seit der letzten Betriebstagung lang.
  - Zu lang um hier auch nur high level aufgeführt zu werden.

Kritische Schwachstellen

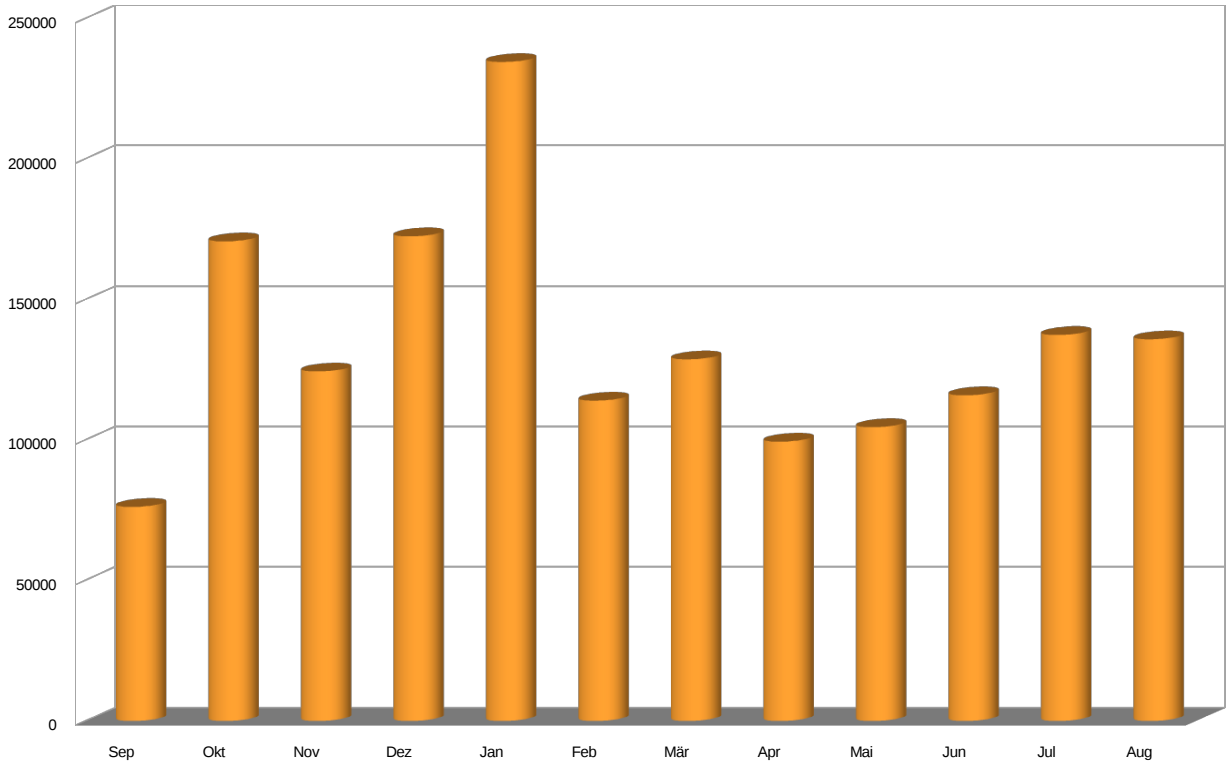
- Kritische und wichtige Sicherheitsupdates sollten eigentlich nicht ohne guten Grund auf die lange Bank geschoben werden.
- Es kann aber natürlich Gründe geben, nicht sofort tätig zu werden. Um dann wenigstens die allerwichtigsten Sicherheitsupdates noch mal ins Gedächtnis zu rufen, habe ich sie in der Vergangenheit im Rahmen der BT in meinem Vortrag aufgeführt.
- Da die Zusammenfassung von sechs Monaten aber so deutlich zu viel ist, möchte ich Ihnen noch einmal unsere DFN-CERT Lageberichte ans Herz legen, die jeweils für den vergangenen Monat die aus unserer Sicht beachtenswertesten Meldungen aufgreifen.

DFN-CERT Lageberichte

- Voraussetzung: Teilnehmer am Dienst DFN-Security
  - Achtung: Nur weil Sie Zugriff auf das Security Portal haben, heißt das **nicht**, dass Sie am Dienst DFN-Security teilnehmen.
  - Das tun Sie nur, wenn Sie die entsprechende Dienstvereinbarung unterschrieben haben.
- Der Bericht ist für Sicherheitskontakte beim jeweiligen Teilnehmer (CISO, Administrierende von Netzbereichen, u. ä.).
- Berechtigung zum Erhalt der Berichte wird geprüft, bevor eine Abonnementwunsch akzeptiert wird, ggf. über Handlungsberechtigte Person.
- Die Berichte sind **nicht** öffentlich!
- Mailingliste: https://www.listserv.dfn.de/sympa/info/dfn-cert-lageberichte

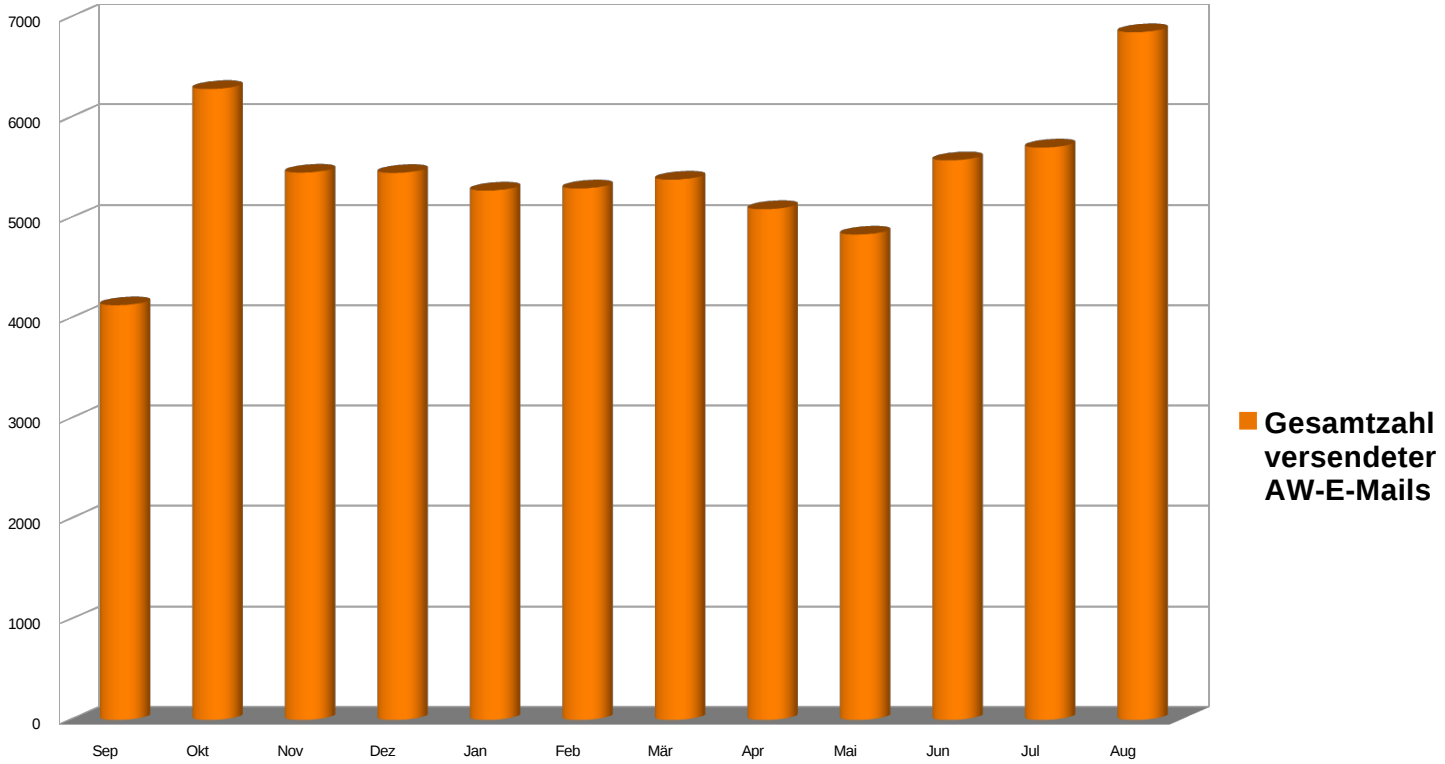
AW-Meldungen

Automatische Warnmeldungen - Events



- März 26:
  - Merklicher Anstieg bei Meldungen zu Systemen, die durch aktuelle Schwachstellen verwundbar waren (Kategorien: `Vulnerabitlity/HTTP`, `Vulnerability/Compromised Website`).
  - Untersuchungen zu Login-Versuchen mit kürzl. erbeuteten Nutzerdaten. Dieselben IP-Adressen auch bei anderen Einrichtungen auffällig.
- April 26:
  - Ende Sept. 2025 kritische, ausgenutzte Schwachstelle in Cisco Secure Firewall Adaptive Security Appliances (ASA) und Threat Defense (FTD). Am 23. April gab es von der U.S. Cybersecurity and Infrastructure Security Agency (CISA) Informationen zu einem dadurch eingeführten, zuvor unbekannten Persistenzmechanismus.

Automatische Warnmeldungen - E-Mails



- Mai 26:
  - CrowdStrike Counter Adversary Operations Team zerschlägt Glassworm-Botnetz. Betroffene Systeme, die mit der Infrastruktur kommunizierten, wurden über die Kategorien `Access/Sinkhole` und `Bot/HTTP` gemeldet.
  - Eine Einrichtung meldete fehlerhaft konfigurierte Firewall, wodurch das System weltweit erreichbar war und diverse Angriffsversuche über eine mögliche Schwachstelle CVE-2026-0300 erfolgten. Vorsorglicher Systemaustausch.
  - Sicherheitsvorfall an der Hochschule Emden/Leer führte zu Abschaltung von IT-Systemen und einem großflächigen Passwortreset.

AW-Meldungen - Vorfälle

- Juni 26:
  - Erhöhte Anzahl von Events in der Kategorie Bot aufgrund kurzzeitig in die Analyse aufgenommener IP-Adresse, die zwar im Zusammenhang mit einer Ransomware-Gruppe aufgefallen ist, aber auch legitime Dienste anbietet.
  - Durch Phishing kompromittierte Daten auf Basis von Recherchen von eye.security werden zukünftig über die Warnmeldungskategorie `Attack/Credentials` weitergegeben.
  - Technische Universität Berlin informierte auf ihrer Webseite über einen Sicherheitsvorfall, der den temporären Ausfall einiger Dienste zur Folge hatte.
- Juli 26:
  - Kompromittierungen von WordPress-Installationen und anderen CMS werden über die Warnmeldungskategorie `Vulnerability/Compromised Website` sowie den zugehörigen Tag `possible-webshell` gemeldet.
  - Über die Warnmeldungskategorie `Vulnerability/Compromised Website` und den Tag `stolen-key` wurden einmalig Daten zu bekannt abgegriffenen ‘Secrets’ von Webseiten verteilt.
  - Das FBI hat in Zusammenarbeit mit Google, Lumen, Shadowserver u. a. das NetNut-Proxy-Netzwerk (Popa), zerschlagen. Kompromittierte Systeme werden über die Warnmeldungskategorie `Access/Sinkhole` gemeldet.
  - Zwei Einrichtungen meldeten die Kompromittierung von jeweils einem System in ihrer Infrastruktur, allerdings ohne weitere Details.

AW-Meldungen - Vorfälle

- August 26:
  - Daten aus dem EU-Projekt AI-Powered Innovative Toolkit for Cybersecurity Hubs (AI-PITCH) werden von Shadowserver in einem Report zu SNMP-Honeypot-Zugriffen verarbeitet. Gemeldet werden Events in der Kategorie `Vulnerability/Honeypot-Access`.
  - Aus dem Bibliotheks-/Katalogumfeld wurde ein DoS-Angriff durch viele unterschiedliche IP-Adressen mit ähnlichen Anfragen gemeldet. (Ziel war hier wohl Ausleitung von Kataloginformationen.) Zur Mitigation: lokale Proof-of-Work-Systeme. Mangels Bandbreite der Angriffe kann das DFN-NOC im Rahmen des DoS-Basisschutzes in der Regel nicht unterstützen.
  - Das Monitoring öffentlich im Klartext verfügbarer Zugangsdaten hat im August einen Datensatz mit 593 Einträgen ergeben, von dem 74 Einrichtungen betroffen waren.
- Dauerbrenner weiterhin
  - Kompromittierte Accounts über die Spam versendet wird
  - und/oder Phishing-Kampagnen stattfinden.

Ankündigungen

Ankündigungen

- MISP Informationsveranstaltung
  - Nächster Termin: **04.11.2026 10:30 -11:30**
  - Einführung in MISP und Information über die Community-Instanz des DFN-CERT
  - Durchgeführt vom DFN-CERT Cyber Threat Intelligence Team
- Virtuelle Informationsveranstaltung DFN-Security
  - Nächster Termin: **03.12.2026 9:30 -12:30**
  - Agenda wird ca. einen Monat vor der Veranstaltung veröffentlicht
  - Wie üblich umfasst der Termin die
    - Vorstellung der Dienstbestandteile
    - Benutzung des Security-Portals
    - Information über die neuesten Änderungen
    - …
- https://www.dfn-cert.de/informationen/veranstaltungen/

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

- DFN-CERT Hotline
  - cert@dfn-cert.de
  - 040 / 808 077-590

Dienst DFN-Security, Security-Portal

portal-contact@dfn-cert.de

DNS-RPZ

dns-rpz@dfn-cert.de

- Weitere Informationen: https://www.security.dfn.de/

https://www.dfn-cert.de/leistungen/security-operations/

