Bundesministerium
Inneres

CERT.at

GovCERT Austria

GovCERT

Sicher. Schnell. Staatlich: Das GovCERT als Cyber-Notruf für Behörden

Sektorspezifisches Computer Notfallteam für
Einrichtungen der öffentlichen Verwaltung

Aufgaben eines Computer-Notfallteams (CERTs bzw. CSIRTs)

4. Abschnitt

Computer-Notfallteams

Aufgaben und Zweck der Computer-Notfallteams

§ 14. (1) Zur Gewährleistung der Sicherheit von Netz- und Informationssystemen werden Computer-Notfallteams eingerichtet. Zu diesem Zweck unterstützen das nationale Computer-Notfallteam und sektorenspezifische Computer-Notfallteams Betreiber wesentlicher Dienste und Anbieter digitaler Dienste sowie das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) die Einrichtungen der öffentlichen Verwaltung bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen.

(2) Computer-Notfallteams gemäß Abs. 1 kommen jedenfalls folgende Aufgaben zu:

1. Entgegennahme von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle gemäß §§ 19, 21 Abs. 2 und 23 Abs. 1 und 2;
2. Weiterleitung von Meldungen (Z 1) an den Bundesminister für Inneres;
3. Ausgabe von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken, Vorfälle oder Sicherheitsvorfälle;
4. Erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;
5. Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen sowie Lagebeurteilung;
6. Teilnahme an den Koordinierungsstrukturen gemäß § 7 und Beteiligung am CSIRTs-Netzwerk.

(3) Betreiber wesentlicher Dienste können für ihren Sektor (§ 2) ein sektorenspezifisches Computer-Notfallteam einrichten, welches die Aufgaben gemäß Abs. 2 gegenüber den Betreibern wesentlicher Dienste, die es unterstützen, wahrnehmen. Sektorenspezifische Computer-Notfallteams können für Zwecke des Abs. 2 Z 3 und 5 im Auftrag eines Betreibers wesentlicher Dienste Daten gemäß § 13 Abs. 1 zweiter Satz analysieren, die durch eine bei diesem Betreiber wesentlicher Dienste eingerichtete IKT-Lösung gemäß § 13 Abs. 1 erster Satz gewonnen wurden. Für Anbieter digitaler Dienste gilt dies mit der Maßgabe, dass sie das nationale Computer-Notfallteam dazu beauftragen können.

(4) Das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) ist beim Bundeskanzler eingerichtet. Neben der Entgegennahme und Weiterleitung von Meldungen gemäß § 22 Abs. 2 und 3, gegebenenfalls gemäß §§ 19 Abs. 2, 21 Abs. 2 und 23 Abs. 3, kommen dem GovCERT die Aufgaben gemäß Abs. 2 Z 3 bis 5 und Abs. 3 zweiter Satz in Hinblick auf die Einrichtungen der öffentlichen Verwaltung, soweit es sich dabei nicht um eine im IKDOK vertretene Einrichtung handelt, zu.

(5) Das GovCERT, das nationale Computer-Notfallteam und die sektorenspezifischen Computer-Notfallteams informieren ohne unnötigen Aufschub den Bundeskanzler sowie den Bundesminister für Inneres über Aktivitäten des CSIRTs-Netzwerks, die zu deren Aufgabenerfüllung nach diesem Bundesgesetz erforderlich sind, und können an dessen Sitzungen teilnehmen.

(6) Computer-Notfallteams können die Aufgaben gemäß Abs. 2 Z 3 bis 5 auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, sofern diese von einem Risiko oder einem Vorfall ihrer Netz- und Informationssysteme betroffen sind.

(7) Computer-Notfallteams sind als datenschutzrechtliche Verantwortliche gemäß Art. 4 Z 7 DSGVO ermächtigt, personenbezogene Daten gemäß § 9 Abs. 2 bis 4 zu verarbeiten, soweit dies zur Erfüllung der Aufgaben gemäß Abs. 2 erforderlich ist.

(8) Computer-Notfallteams sind zur Wahrnehmung der Aufgaben gemäß Abs. 2 Z 3, 5 und 6 berechtigt, personenbezogene Daten gemäß § 9 Abs. 2 Z 2 und Abs. 3 Z 2 an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste, Einrichtungen der öffentlichen Verwaltung, Einrichtungen, die gemäß § 23 Abs. 2 gemeldet haben und an Teilnehmer des CSIRTs-Netzwerks sowie einander zu übermitteln.

GovCERT Austria

Bundesministerium
Inneres

CERT.at

GovCERT – Beispiel f. Frühwarnung und Unterstützung

- Beispiel anhand einer aktiv ausgenutzten Schwachstelle im Software-Produkt Ivanti Endpoint Manager Mobile (EPMM)

Taegliche Neuigkeiten von GovCERT.gv.at

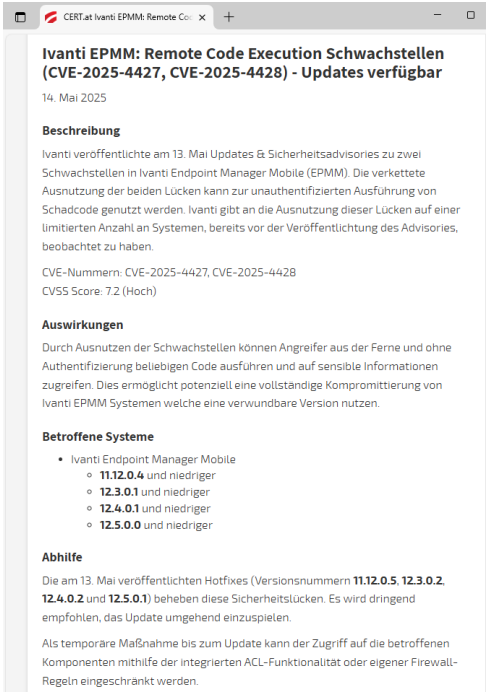
```
======================
= End-of-Day report =
======================

Timeframe:   Dienstag 13-05-2025 18:00 – Mittwoch 14-05-2025 18:01
Handler:     Michael Schlagenhaufer
Co-Handler:  Guenes Holler

======================
= Vulnerabilities =
======================

*** Ivanti EPMM: Remote Code Execution Schwachstellen (CVE-2025-4427, CVE-2025-4428) - Updates verfügbar ***
------------------------------------------------
Ivanti veröffentlichte am 13. Mai Updates & Sicherheitsadvisories zu zwei Schwachstellen in Ivanti Endpoint Manager Mobile (EPMM). Die verkettete Ausnutzung der beiden Lücken kann zur unauthentifizierten Ausführung von Schadcode genutzt werden. Ivanti gibt an die Ausnutzung dieser Lücken auf einer limitierten Anzahl an Systemen, bereits vor der Veröffentlichung des Advisories, beobachtet zu haben. CVE-Nummern: CVE-2025-4427, CVE-2025-4428
------------------------------------------------
https://www.cert.at/de/warnungen/2025/5/ivanti-epmm-rce
```

1. rasche **Warnung** per Mailinglist
2. weiterführende Information und **Abhilfe** via Website durch CERT.at
3. automatische technische **Information** durch CERT.at-„MISP“-Server
4. Option der Hinterlegung von Kontaktdaten bei CERT.at



CERT.at Ivanti EPMM: Remote Co

Ivanti EPMM: Remote Code Execution Schwachstellen (CVE-2025-4427, CVE-2025-4428) - Updates verfügbar

14. Mai 2025

Beschreibung

Ivanti veröffentlichte am 13. Mai Updates & Sicherheitsadvisories zu zwei Schwachstellen in Ivanti Endpoint Manager Mobile (EPMM). Die verkettete Ausnutzung der beiden Lücken kann zur unauthentifizierten Ausführung von Schadcode genutzt werden. Ivanti gibt an die Ausnutzung dieser Lücken auf einer limitierten Anzahl an Systemen, bereits vor der Veröffentlichung des Advisories, beobachtet zu haben.

CVE-Nummern: CVE-2025-4427, CVE-2025-4428
CVSS Score: 7.2 (Hoch)

Auswirkungen

Durch Ausnutzen der Schwachstellen können Angreifer aus der Ferne und ohne Authentifizierung beliebigen Code ausführen und auf sensible Informationen zugreifen. Dies ermöglicht potenziell eine vollständige Kompromittierung von Ivanti EPMM Systemen welche eine verwundbare Version nutzen.

Betroffene Systeme

- Ivanti Endpoint Manager Mobile
  - **11.12.0.4** und niedriger
  - **12.3.0.1** und niedriger
  - **12.4.0.1** und niedriger
  - **12.5.0.0** und niedriger

Abhilfe

Die am 13. Mai veröffentlichten Hotfixes (Versionsnummern **11.12.0.5**, **12.3.0.2**, **12.4.0.2** und **12.5.0.1**) beheben diese Sicherheitslücken. Es wird dringend empfohlen, das Update umgehend einzuspielen.

Als temporäre Maßnahme bis zum Update kann der Zugriff auf die betroffenen Komponenten mithilfe der integrierten ACL-Funktionalität oder eigener Firewall-Regeln eingeschränkt werden.

GovCERT

- lt. Geschäftsordnung des GovCERTs: § 6 „Teilnahme am Informationsaustausch“
  - Die Organisation benennt **zwei Kontaktpersonen** (Points of Contact) als offizielle Ansprechpartner gegenüber GovCERT. → govcert@lists.govcert.gv.at
  - Die offiziellen Ansprechpartner können weitere Personen des/der jeweiligen **technischen Teams** dem GovCERT bekannt geben. → govcert-e@lists.govcert.gv.at
  - Beim Informationsaustausch wird bei Bedarf die Sensitivität der geteilten Information gekennzeichnet, z.B. durch das **Traffic Light Protocol**. Bei Bedarf wird genauer erläutert, wie die Informationen verwendet werden dürfen.
- Das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) ist **beim Innenminister eingerichtet**.
- Die operative Tätigkeit wird durch **CERT.at** erbracht

CNW – CSIRTs Network

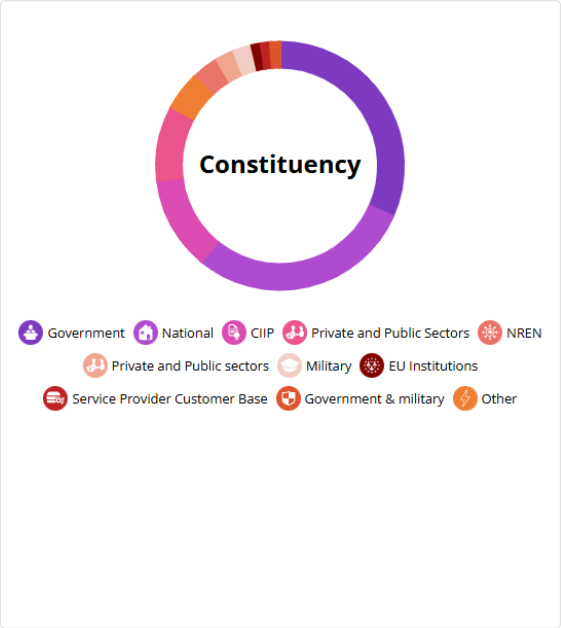
Das CNW der Europäischen Union ist ein Netzwerk, das sich aus den von den EU-Mitgliedstaaten benannten CSIRTs und dem CERT-EU zusammensetzt

CNW – CSIRTs Network

- Ziel des **durch die NIS-Richtlinie 1 eingerichteten** und durch die NIS-Richtlinie 2 gestärkten CSIRTs-Netzwerks ist es, „zur **Entwicklung von Vertrauen** zwischen den Mitgliedstaaten beizutragen und eine **rasche und wirksame operative Zusammenarbeit** zu fördern“.
- Das CSIRTs-Netz ist ein Netzwerk, in dem die Mitglieder des CSIRTs-Netzes zusammenarbeiten, Informationen austauschen, den Umgang mit **grenzüberschreitenden Vorfällen** verbessern und auf bestimmte Vorfälle **koordiniert reagieren**.
- **Das CSIRTs-Netz besteht aus den von den EU-Mitgliedstaaten benannten CSIRTs und CERT-EU** („CSIRTs-Netzmitglieder“).Die ENISA stellt das Sekretariat, die Infrastrukturen und die Instrumente für eine wirksame Zusammenarbeit zur Verfügung.

CNW – CSIRTs Network

- Das CNW bietet allen Computer Notfallteams der EU eine Plattform für den schnellen **Informationsaustausch** in einem **vertrauenswürdigen Rahmen**



- Treffen 2x pro Jahr
- Letztes Meeting im Mai, Teilnahme vor Ort durch BMI + Cert.at

Teaser: EU Cybersecurity Reserve

- https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cybersecurity-reserve
- Etabliert durch den EU Cyber Solidarity Act (seit Feb. 25 in Kraft)
- Abwicklung durch Unterstützung von CSIRTS

GovCERT – Kontakt

Fazit:

Informationsaustausch ist Key – bringe die richtige Information, zur richtigen Zeit an die richtige Stelle!

Durch Vernetzung, Vertrauen und Kooperation

team@govcert.gv.at