16/2020

22. April 2020

Cybersecurity: CERT@VDE zur “CVE Numbering Authority” (CNA) benannt

- **Aufnahmeprozess erfolgreich absolviert: Das CVE-Programm nimmt CERT@VDE in die CVE-Community auf**
- **CERT@VDE vergibt nun CVE-IDs für Schwachstellen in Produkten von Herstellern der Automatisierungsindustrie und ermöglicht Prozessoptimierung im Schwachstellenmanagement**

(Frankfurt a.M., Deutschland / McLean, Virginia, USA, 22.04.2020) Die Experten des CERT@VDE haben den Anerkennungsprozess als “CVE Numbering Authority” (CNA)” des global anerkannten Common Vulnerabilities and Exposures (CVE) Programms erfolgreich bestanden und sind damit autorisiert, CVE-Nummern für Cyber-Sicherheitslücken in den Produkten der CERT@VDE-Partner sowie der Automatisierungsbranche zuzuweisen und in das öffentlich zugängliche CVE-Register zu integrieren. „Das CVE-Programm freut sich, dass die Expertise des CERT@VDE zu den globalen Bemühungen um die Identifizierung von Schwachstellen beiträgt. Als autorisierte CNA trägt CERT@VDE zum Kampf der globalen Cyber-Sicherheitsgemeinschaft gegen Cyber-Kriminelle bei", kommentiert Kent Landfield, McAfee und CVE-Vorstandsmitglied.

Schnelle Identifikation von Cyber-Sicherheitslücken

Die CVE-Konvention zur Benennung von Schwachstellen ist ein internationaler De-facto-Standard. Sie schreibt für jede Cyber-Sicherheitslücke eine eindeutige CVE-Nummer vor, um sicherzustellen, dass sie eindeutig spezifiziert ist. Mit der Benennung zur CNA helfen die Experten von CERT@VDE ihren Partnern, Schwachstellen schnell zu identifizieren und zu beheben, um Cyberkriminellen keine Angriffsfläche zu bieten. „Nichts ist fataler als eine Mehrfachbenennung ein und desselben Cybersecurity-Problems. Wir kooperieren mit Experten – Hackern und Forschern – rund um den Globus und würden so wertvolle Zeit beim Informationsaustausch verschwenden“, erklären Andreas Harner, Jochen Becker und Christian Link vom CERT@VDE.

Schutz gegen Hackerangriffe: Prozessoptimierung im Schwachstellenmanagement

Cybersecurity-Experten sind sich weltweit einig: Schwachstellen und Sicherheitslücken in Software-Produkten haben unterschiedlichste Ursachen und werden aufgrund dessen niemals ganz verschwinden. Eine einheitliche Namenskonvention für Sicherheitslücken ist daher essenziell, um der wachsenden Zahl von Schwachstellen überhaupt noch Herr zu werden. Aus diesem Grund verwaltet die MITRE Corporation in Zusammenarbeit mit mehr als 100 CNA-Partnern weltweit die CVE-Nummern. „Und zu dieser Community gehört nun auch das CERT@VDE“, freut sich Andreas Harner, Leiter CERT@VDE, und ergänzt: „Wir erkennen einen exponentiellen Anstieg von entdeckten Schwachstellen, die Hacker ausnutzen könnten, um deutsche Unternehmen anzugreifen.“ Die Anerkennung als CNA ist ein wichtiger Schritt, um durch Prozessoptimierung eine noch größere Wertschöpfung im Schwachstellenmanagement für die CERT@VDE Mitglieder zu erzielen. „CVE verdeutlicht, wie wichtig Standardisierung im CERT-Bereich und im Kampf gegen Cyberkriminelle heute schon ist“, erklärt auch Michael Teigeler, Geschäftsführer von VDE|DKE.

Über den VDE:

Der VDE, eine der größten Technologie-Organisationen Europas, steht seit mehr als 125 Jahren für Innovation und technologischen Fortschritt. Als einzige Organisation weltweit vereint der VDE dabei Wissenschaft, Standardisierung, Prüfung, Zertifizierung und Anwendungsberatung unter einem Dach. Das VDE-Zeichen gilt seit 100 Jahren als Synonym für höchste Sicherheitsstandards und Verbraucherschutz. Wir setzen uns ein für die Forschungs- und Nachwuchsförderung und für das lebenslange Lernen mit Weiterbildungsangeboten „on the job“. 2.000 Mitarbeiter an über 60 Standorten weltweit, mehr als 100.000 ehrenamtliche Experten und rund 1.500 Unternehmen gestalten im Netzwerk VDE eine lebenswerte Zukunft: vernetzt, digital, elektrisch. Wir gestalten die e-diale Zukunft.

Hauptsitz des VDE (Verband der Elektrotechnik Elektronik und Informationstechnik e.V.) ist Frankfurt am Main. Mehr Informationen unter www.vde.com.

Pressekontakt: Melanie Unseld, Tel. 069 6308461, melanie.unseld@vde.com

Glossar:

CVE: Common Vulnerabilities and Exposures (deutsch: Gemeinsame Schwachstellen und Enthüllungen): Industriestandard, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und Schwachstellen in Computer- und IoT-Systemen ist.

CNA: CVE Numbering Authority (deutsch: CVE-Nummerierungsbehörde): CNAs sind Organisationen aus der ganzen Welt, die berechtigt sind, CVE-IDs für Schwachstellen, die Produkte innerhalb ihres eigenen, vereinbarten Geltungsbereichs betreffen, zur Aufnahme in erstmalige öffentliche Bekanntmachungen neuer Schwachstellen zu vergeben. Diese CVE-IDs werden Forschern, Offenlegern von Schwachstellen und Anbietern von Informationstechnologie zur Verfügung gestellt.

CERT: Computer Emergency Response Team (deutsch: Computersicherheits-Ereignis- und Reaktionsteam): Team von Sicherheitsexperten und Cybersecurity-Fachleuten. Sie wirken an der Lösung von konkreten Sicherheitsvorfällen mit, liefern Lösungsansätze oder warnen vor Sicherheitslücken.

MITRE Corporation: ist eine gemeinnützige Organisation zum Betrieb von Forschungseinrichtungen im Auftrag der USA, die durch Abspaltung vom Massachusetts Institute of Technology (MIT) entstanden ist. MITRE verwaltet zudem die Liste der Common Vulnerabilities and Exposures (CVE).