



16/2020

April 20, 2020

Cybersecurity: CERT@VDE named "CVE Numbering Authority" (CNA)

- **Admission process successfully completed: The CVE Program admits CERT@VDE to the CVE - Community**
- **CERT@VDE now assigns CVE-IDs for vulnerabilities in products of automation industry manufacturers and enables process optimization in vulnerability management**

(Frankfurt a.M., Germany / McLean, Virginia, USA, April 20, 2020) The experts of CERT@VDE have successfully passed the recognition process as "CVE Numbering Authority" (CNA) of the globally recognized Common Vulnerabilities and Exposures (CVE) program. They are now authorized to assign CVE numbers for vulnerabilities in the products of the CERT@VDE partners, as well as the automation industry, and to integrate them into the publicly accessible CVE-registry. "The CVE Program is happy to have the expertise of the CERT@VDE contributing to the global vulnerability identification efforts. As an authorized CNA, CERT@VDE is adding value to the global cybersecurity community's battle against cyber criminals", comments Kent Landfield, McAfee and CVE Board Member

Fast identification of vulnerabilities

The CVE vulnerability naming convention is an international de facto standard. It requires a unique CVE number for each cyber security gap to ensure that it is uniquely specified. By naming them CNAs, the experts at CERT@VDE are supporting the global good by identifying vulnerabilities and assigning CVE-ids, while helping their partners in eliminate vulnerabilities so that cybercriminals cannot attack them. "Nothing is more fatal than the multiple designation of one and the same cybersecurity problem. We cooperate with experts - hackers and researchers - around the globe and would thus waste valuable time in exchanging information", comment Andreas Harner, Jochen Becker and Christian Link from CERT@VDE.

Protection against hacker attacks: Process optimization in vulnerability m management

Cybersecurity experts all over the world agree: weaknesses and security gaps in software products have a wide variety of causes and will therefore never completely disappear. A uniform naming convention for security vulnerabilities is therefore essential if the growing number of vulnerabilities is to be controlled in the future. For this reason, the MITRE Corporation manages CVE numbers in cooperation with more than 100 CNA partners worldwide. "And CERT@VDE is now part of this community," says Andreas Harner, head of CERT@VDE, happily, adding: "We are seeing an exponential increase in the number of discovered vulnerabilities that hackers could exploit to attack German companies." The recognition as CNA is an important step to achieve even greater added value in vulnerability management for CERT@VDE members through process optimization. "CVE illustrates how important standardization in the CERT area and in the fight against cybercriminals already is today", explains Michael Teigeler, Managing Director of VDE|DKE.

About VDE:

VDE, one of the largest technology organizations in Europe, has been regarded as a synonym for innovation and technological progress for more than 125 years. VDE is the only organization in the world that combines science, standardization, testing, certification, and application consulting under one umbrella. The VDE mark has been synonymous with the highest safety standards and consumer protection for 100 years. Our passion is the advancement of technology, the next generation of engineers and technologists, and lifelong learning and career development "on the job". Within the VDE network 2,000 employees at over 60 locations worldwide, more than 100,000 honorary experts, and 1,500 companies are dedicated to ensuring a future worth living: networked, digital, electrical. We shape the e-dialistic future. The headquarters of the VDE (Association for Electrical, Electronic & Information Technologies) is in Frankfurt am Main. www.vde.com

Contact: Melanie Unseld, Spokesperson VDE, +49 175 1874333, melanie.unseld@vde.com

Glossary:

CVE: Common Vulnerabilities and Exposures: Industry standard that aims to establish a common naming convention for vulnerabilities and exposures in computer and IoT systems.

CNA: CVE Numbering Authority: CVE Numbering Authorities (CNAs) are organizations from around the world that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed-upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVE IDs are provided to researchers, vulnerability disclosers, and information technology vendors

CERT: Computer Emergency Response Team: Team of security experts and cybersecurity professionals. They participate in the resolution of specific security incidents, provide solutions or warn of security breaches.

MITRE Corporation: is a nonprofit organization that operates research facilities on behalf of the U.S. that was formed by a spin-off from the Massachusetts Institute of Technology (MIT). MITRE also manages the Common Vulnerabilities and Exposures (CVE) list.