Schubladen für Schwachstellen: Das CVE-System im Überblick

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>Schubladen für Schwachstellen: Das CVE-System im Überblick</h1> Olivia von Westernhagen </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: MIA Studio / Shutterstock.com (Collage))</figcaption></figure> MITREs Common Vulnerabilities and Exposures System (CVE) ist der gängige Standard zur Verwaltung von Schwachstellen. Wir erklären, was es damit auf sich hat. Bereits im letzten Jahrtausend gestaltete sich die Kommunikation über Sicherheitslücken zunehmend schwierig: Wer von „die Sicherheitslücke im Internet Explorer“ sprach, adressierte oftmals mehr als ein Dutzend aktueller Bugs. Eingrenzungen à la „die Lücke mit ActiveX“ halfen kaum weiter, da das immer noch auf viele zutraf. Um Missverständnisse zu vermeiden und sicherzustellen, dass alle vom gleichen Problem sprachen, musste eine herstellerübergeifende, einheitliche Strategie zur Erfassung und Verwaltung von Schwachstellen her. 1999 begann man daher mit einer systematischen Durchnummerierung: Das CVE (Common Vulnerabilities and Exposures)-System war geboren und hat sich seither als weltweit führender Industriestandard durchgesetzt. Betreut und verwaltet wird es von der gemeinnützigen MITRE Corporation, finanziert mit Mitteln der US-Sicherheitsbehörden CISA (Cybersecurity and Infrastructure Security Agency) und DHS (Department of Homeland Security). <h3 class=„subheading“ id=„nav_cve_yyyy_nnnnn_0“>CVE-YYYY-NNNNN</h3> CVE-Nummern beziehungsweise -IDs im Format CVE-YYYY-NNNNN dürften jedem schonmal begegnet sein, der sich mit Schwachstellen befasst hat – etwa auf der Suche nach Sicherheitsupdates für ein bestimmtes Produkt oder auch beim Lesen von Alerts bei heise Security. Auf das „CVE“ am Anfang folgt stets eine Jahresangabe. Bei dieser handelt es laut MITRE allerdings nicht (unbedingt) um das Jahr, in dem die Lücke entdeckt, sondern vielmehr um jenes, in dem sie publik gemacht beziehungsweise in dem die Nummer vergeben wurde. Der letzte Teil der ID mit der eigentlichen Nummer war mit Einführung des CVE-Systems Ende 1999 noch auf vier Ziffern beschränkt. Da 9999 mögliche einzigartige IDs pro Jahr irgendwann aber nicht mehr ausreichten, wurde die Syntax Anfang 2014 geändert [1]. Eine maximale Länge des „NNNNN“-Parts der IDs gibt es nun nicht mehr; sie orientiert sich am Bedarf im jeweiligen Kalenderjahr. Lediglich das Minimum wurde auf vier Ziffern festgeschrieben. <h3 class=„subheading“ id=„nav_id_vergabe1“>ID-Vergabe durch CNAs</h3> Natürlich sorgt eine einheitliche Syntax allein nicht für Ordnung. Damit CVE-IDs nicht unkontrolliert vergeben werden, haben

nur bestimmte Personen, Organisationen und Unternehmen, so genannte CVE Numbering Authorities (CNAs), die Befugnis zur CVE-Vergabe. Diese wiederum teilen die Zuständigkeit für verschiedene Produkte und Projekte klar unter sich auf. Übergeordnete (Top-Level) Root CNAs, sind derzeit das MITRE CVE-Team, CISA und und das japanische JPCERT/CC. Ihnen untergeordnet sind „normale“ CNAs, deren Befugnisse unterschiedlich weit reichen können. So befinden sich darunter etwa Soft- und Hardware-Hersteller, die CVE-IDs nur für ihre eigenen Produkte vergeben dürfen, aber auch CERTs, die die Vergabe für jeweils mehrere Unternehmen koordinieren. Unabhängige Forscher, Forscherteams oder IT-Sicherheitsunternehmen (z.B. die Zero Day Initiative oder auch Rapid7) können, teilweise im Rahmen von Bug Bounty-Programmen, auch herstellerübergreifend als CNA für Produkte agieren, die nicht im Verantwortungsbereich einer anderen CNA liegen. Ähnliches gilt für so genannte CNAs of Last Resort (CNA-LR). Wer eine Schwachstelle in einem bestimmten Produkt entdeckt und diese melden will, findet die jeweils zuständige Anlaufstelle in einer CNA-Übersicht auf MITREs CVE-Website [2]. Die CNA kümmert sich im nächsten Schritt um die Reservierung einer CVE-ID. Die landet in MITREs fortlaufend geführter CVE-Liste [3]– typischerweise zunächst mit dem Vermerk „Reserved“. Später vervollständigen eine Schwachstellen-Beschreibung und meist auch Verlinkungen zu weiterführenden Informationen den CVE-Eintrag. <h3 class=„subheading“ id=„nav_cve_nutzun2“>CVE-Nutzung durch heise Security</h3> Auch heise Security verwendet wo immer es sinnvoll möglich ist CVE-Nummern. Wir betten diese etwa in unsere Alert-Meldungen mit ein, um später eine gezieltes Suche nach einer bestimmten Lücke zu ermöglichen. Die Links auf die eigentlichen CVE-Seiten bringen zum Zeitpunkt, zu dem unsere Meldungen erscheinen, oftmals nur wenig Mehrwert, da sich die ID mitunter noch im „Reserved“-Status befindet. Um unsere Leser nicht in diese Sackgasse zu schicken, lassen wir die Links daher auch häufig weg und erwähnen lediglich die CVE-Nummer. Bei Sammeladvisories beschränken wir uns auf die zentralen Lücken, die in der weiteren Berichterstattung am wahrscheinlichsten eine Rolle spielen werden. Sonst müssten wir etwa bei einem Oracle Critical Patch Update mal eben 400 IDs in unsere Artikel pressen – und der Mehrwert für unsere Leser wäre gleich Null. <h3 class=„subheading“ id=„nav_zusatz_inf3“>Zusatz-Infos in der NVD</h3> Sind dagegen bereits weiterführende Informationen verfügbar, bieten sich statt einer Verlinkung auf MITREs CVE-Liste alternativ auch Verweise auf die so genannte National Vulnerability Database (NVD) [4] an. Sie ist ein unabhängiges, 2005 vom National Institute of Standards and Technology (NIST) ins Leben gerufenes Projekt, das wie das CVE-System von den US-Behörden CISA und DHS gesponsert wird. Die NVD speist sich aus MITREs CVE-Liste, fügt den eher knappen Beschreibungen allerdings wertvolle Zusatzinformationen etwa zu Sicherheitsrisiken oder verfügbaren Updates hinzu. Zur einheitlichen Beschreibung von Schwachstellen-Eigenschaften nutzt (nicht nur) die NVD wiederum ein spezielles System, mit dem unter anderem man einen Schweregrad von „Low“ bis „Critical“ zuweisen und Aussagen zu Angriffsweg, -komplexität und Co. anhand vordefinierter Kriterien treffen kann. Dieses so genannte Common Vulnerability Scoring System (CVSS) hat einen eigenen Hintergrundartikel verdient, der demnächst bei heise Security erscheinen soll. <header class=„a-boxheader“ data-collapse-trigger=„“>Lesen Sie auch</header><div class=„a-boxtarget a-boxcontent“ data-collapse-target=„“><article class=„a-article-teaser a-article-teaser–horizontal-layout article-teaser–articlebox a-u-no-margin-bottom a-theme“ data-cid=„0“><figure

class=„a-article-teaserimage-container“> </figure> <header><h1 class=„a-article-teasertitle a-u-mb-1“>Orientierung im Security-Babylon</h1></header> [5]</article> () <hr /> URL dieses Artikels:
<small><code>https://www.heise.de/-4940478</code></small> Links in diesem Artikel:
<small><code>[1] https://cve.mitre.org/news/archives/2014/news.html#jan152014_New_CVE_ID_Format_in_Effect_as_of_January_1_2014</code></small>
<small><code>[2] https://cve.mitre.org/cve/request_id.html</code></small>
<small><code>[3] https://cve.mitre.org/index.html</code></small>
<small><code>[4] https://nvd.nist.gov/</code></small>
<small><code>[5] https://www.heise.de/hintergrund/Orientierung-im-Security-Babylon-4892855.html</code></small>
<small><code>[6] mailto:ovw@heise.de</code></small>
 Copyright © 2020 Heise Medien </html>