Baden-Württemberg

LANDESKRIMINALAMT

Warnmeldung für Firmen und Behörden

Cyberangriff auf FireEye

Mögliche Ausnutzung von Sicherheitslücken mittels bei der Firma FirEye entwendeten Tools

Stuttgart, 11.12.2020

Die US-amerikanische IT-Sicherheitsfirma ist nach eigener Auskunft[1] Opfer eines Cyberangriffes geworden. FireEye ist eine renommierte und weltweit tätige IT-Sicherheitsfirma, zu deren Leistungsspektrum unter anderen Penetrationstests gehören. Hierbei setzt FireEye auch selbstentwickelte Tools und Methoden ein, mit denen Sicherheitslücken in IT-Systemen automatisiert gefunden werden können.
Im Rahmen des Cyberangriffes auf FireEye wurden solche Tools entwendet.

Von FireEye wurden umfangreiche Hintergrundinfos zu den entwendeten Werkzeugen und den ausgenutzten Sicherheitslücken veröffentlicht.[2] Auch wenn sämtliche entwendete Werkzeuge auf bekannte Sicherheitslücken referenzieren, für welche bereits Sicherheitsupdates zur Verfügung stehen, besteht die Gefahr, dass diese Sicherheitslücken aktuell gezielt von Cyberkriminellen gesucht und ausgenutzt werden.

Neben der grundsätzlichen Empfehlung, sämtliche IT-Systeme auf dem aktuellsten Softwarestand zu halten und Updates zeitnah einzuspielen, wird daher dringend

[1] https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cy-ber-attack-actions-to-protect-community.html
[2] https://github.com/fireeye/red_team_tool_countermeasures

empfohlen, die IT-Systeme hinsichtlich folgender Sicherheitslücken zu überprüfen und zeitnah die von Herstellern zur Verfügung gestellten Sicherheitsupdates zu installieren:

- CVE-2014-1812 – Windows Local Privilege Escalation
- CVE-2019-0708 – RCE of Windows Remote Desktop Services (RDS)
- CVE-2017-11774 – RCE in Microsoft Outlook via crafted document execution (phishing)
- CVE-2018-15961 – RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)
- CVE-2019-19781 – RCE of Citrix Application Delivery Controller and Citrix Gateway
- CVE-2019-3398 – Confluence Authenticated Remote Code Execution
- CVE-2019-11580 – Atlassian Crowd Remote Code Execution
- CVE-2018-13379 – pre-auth arbitrary file reading from Fortinet Fortigate SSL VPN
- CVE-2020-0688 – Remote Command Execution in Microsoft Exchange
- CVE-2019-11510 – pre-auth arbitrary file reading from Pulse Secure SSL VPNs
- CVE-2019-0604 – RCE for Microsoft Sharepoint
- CVE-2020-10189 – RCE for ZoHo ManageEngine Desktop Central
- CVE-2019-8394 – arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDeskPlus
- CVE-2016-0167 – local privilege escalation on older versions of Microsoft Windows
- CVE-2020-1472 – Microsoft Active Directory escalation of privileges
- CVE-2018-8581 – Microsoft Exchange Server escalation of privileges

Von FireEye wurden darüber hinaus umfangreiche Metriken veröffentlicht, mittels derer entsprechende Schadprogramme innerhalb der IT-Infrastruktur detektiert werden können. Diese finden sich ebenfalls auf der genannten Github-Seite.

Weitere Informationen zu den aufgeführten Sicherheitslücken (CVEs) finden Sie unter www.cve.mitre.org

Zentrale Ansprechstelle Cybercrime
beim Landeskriminalamt Baden-Württemberg

Die ZAC dient als zentraler Ansprechpartner für die Wirtschaft und Behörden in allen Belangen des Themenfeldes Cybercrime.

Erreichbarkeit der ZAC:
Telefon: +49 (0)711 5401 2444
E-Mail: **cybercrime@polizei.bwl.de**
Website: www.lka-bw.de/zac