Einsatz von Linux bei der Entwicklung sicherer Medizinprodukte

Ein Betriebssystem wie Linux ist kein Safety-Mechanismus. Es ermöglicht jedoch die Anwendungen und wird als Safety-Element betrachtet.

Das Open-Source-Betriebssystem (BS) Linux wird in einer Vielzahl von Medizinprodukten eingesetzt. Sowohl Safety als auch Security sind bei der Entwicklung von Medizinprodukten notwendig, doch nicht alle Aspekte der Safety sind mit Security verbunden. Wenn das Medizinprodukt nicht secure ist, können Hacker das Geschehen negativ beeinflussen – mit ernsthaften Folgen für die Sicherheit und das Wohlbefinden des Patienten.

Linux ist das weltweit am meisten für Geräte genutzte BS und die Linux-Entwicklerbasis sorgt dafür, dass es unter allen Bedingungen einwandfrei und mit größtmöglicher Security funktioniert. Embedded-Entwickler arbeiten verantwortungsbewusst an der Verbesserung von Linux und anderen Open-Source-Paketen, doch es gibt Hacker, die versuchen, in Linux einzudringen, um ihre eigenen Zwecke zu verfolgen. Die Security von Open-Source-Anwendungen ist durch das ständige Tauziehen zwischen diesen entgegengesetzten Kräften geprägt.

Unvorhersehbares Verhalten

Linux (und andere bedeutende BS-Pakete wie OpenSSL oder SQLite) können auf unvorhersehbare Weise mit anderer Software im System interagieren. Viele Softwarefehler sind bei Codeüberprüfungen, üblichen Tests oder durch statische Analyse nur schwer fassbar. Sie lassen sich nicht nachweisen, außer wenn die Software mit Taskwechseln und Interprozesskommunikation kombiniert wird.

Kritische Elemente werden sicherer

Kritische Elemente von Open-Source-Software in Medizinprodukten weltweit sind heute wesentlich stabiler und sicherer. Dies ist der harten Arbeit und Sorgfalt von Global Engineers zu verdanken, die Wege zur Ausnutzung von Schwachstellen identifizieren und gefundene beseitigen, sowie der weltweiten Community, die in Verbindung mit eigenen Projekten solche Probleme aufspühren. Es ist schwieriger geworden, ausnutzbare Schwachstellen zu finden, aber es bleibt weiterhin eine laufende Aufgabe.

Linux-Sicherheitsprobleme (einschließlich Software wie OpenSSL) werden in der Regel von Ingenieuren gefunden, zum Beispiel Fehler, die im Rahmen der täglichen Arbeit aufgedeckt werden. Manchmal wird ein Exploit bei der Postmortem-Analyse eines Angriffs gefunden. Normalerweise benachrichtigt der Entdecker oder ein Mitglied der Community die Common Vulnerability and Exposures (CVE) Gruppe. Diese wird von der MITRE betrieben, einer Organisation im Auftrag der Vereinigten Staaten, die in Beziehung zur National Vulnerability Database (NVD) steht, ihrerseits betrieben vom National Institute of Standards and Technology (NIST).

Umgang mit Schwachstellen

Wenn eine Schwachstelle gefunden wurde und eine Lösung zur Behebung vorliegt, wird die CVE veröffentlicht. Schwerwiegende Probleme werden in der Security-Community weltweit diskutiert. Das ist die Phase, in der Medizinprodukte potenziell am meisten gefährdet sind. Die „Bösen“ können sich über sie informieren (wie der Rest der Welt) und von der neu entdeckten Schwachstelle profitieren. Die Veröffentlichung ist jedoch von entscheidender Bedeutung, denn sie informiert die internationale Community über das Problem und seine Lösung. Unternehmen können daraufhin ermitteln, ob sich dieser bestimmte Exploit auf ihre Produkte auswirken könnte. Wenn ja, können sie dem Problem entgegenwirken, bevor es eventuell zu einem Angriff kommt. ◄

Autor:
Scot Morrison ist General Manager der allgemeinen Embedded-Geschäftseinheit, Mentor Embedded Systems Division.
Mentor, a Siemens Business
www.mentor.com

Weitere Informationen unter https://www.mentor.com/embedded-software/linux/