Zehn Sicherheitslücken in McAfee VirusScan Enterprise Linux geschlossen

Intel Security hat gestern zehn Sicherheitslücken in seiner Sicherheitssoftware VirusScan Enterprise for Linux/LinuxShield geschlossen. Betroffen ist davon Version 2.0.3 und früher. Das Unternehmen empfiehlt Nutzern den Umstieg auf Endpoint Security for Linux (ENSL) 10.2.

Das Update wirft nicht nur angesichts der Anzahl der Lücken kein gutes Licht auf den Anbieter, sondern auch aufgrund der Zeit, die es gedauert hat, bis sie endlich geschlossen wurden. Andrew Fasano vom MIT Lincoln Laboratory hatte das Unternehmen bereits am 23. Juni darüber informiert. Die eigentlich für 23. August vorgesehene Veröffentlichung seiner Erkenntnisse hat er dann auf Bitten des Unternehmens verschoben.

Laut Fasano lassen sich die Schwachstellen so kombinieren, dass am Ende Angreifer als Root-Administrator Code aus der Ferne ausführen können – also letztendlich jede beliebige Aktion möglich ist. Dazu trägt auch bei, dass die Sicherheitslücken es Angreifern erlauben, von ihnen kontrollierte Update-Server aufzusetzen und die Software dazu bringen können, sich von dort mit manipulierten Aktualisierungen zu versorgen.

Um die Schwachstellen auszunutzen, können Angreifer über die Sicherheitslücken mit den Kennungen CVE-2016-8022 und CVE-2016-8023 zunächst das Authentifizierungs-Token per Brute-Force-Attacke knacken und es dann verwenden, um sich mit den McAfee Linux Clients zu verbinden. Die Lücke mit der Kennung CVE-2016-8021 erlaubt es ihnen anschließend, manipulierte Skripte zu installieren. Über dieselbe Lücke ist es danach möglich, zusammen mit einer unautorisierten Rechteausweitung (Kennung CVE-2016-8021) den eingeschleusten Code mit Root-Rechten auszuführen. Details der vier als hohes Risiko eingestuften Lücken und der restlichen Schwachstellen beschreibt Entdecker Fasano ausführlich.