Schwachstelle in ESET-Antivirus-Produkten

ESET wurde von der Zero Day Initiative (ZDI) über eine lokale Schwachstelle informiert, die zu einer Ausweitung der Berechtigungen führt. Die Schwachstelle ermöglicht es einem Angreifer, die vom Echtzeit-Dateisystemschutz von ESET durchgeführten Dateioperationen zu missbrauchen, um Dateien ohne entsprechende Berechtigung zu löschen.

Um was geht es?

Die Zero Day Initiative (ZDI) hat ESET einen Bericht über eine lokale Sicherheitslücke bei der Eskalation von Berechtigungen übermittelt. Die Sicherheitslücke ermöglicht es einem Angreifer möglicherweise, die Dateivorgänge von ESET zu missbrauchen, um Dateien zu löschen, ohne über die entsprechende Berechtigung zu verfügen. Dabei wird die Schwachstelle der Komponente vom Echtzeit-Dateisystemschutz ausgenutzt.

Schwachstelle:
CVE-2024-0353

Betroffene Produkt Versionen:

- ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security Premium, ESET Security Ultimate 16.2.15.0 und höher
- ESET Endpoint Antivirus für Windows und ESET Endpoint Security für Windows 10.1.2058.0, 10.0.2049.0, 9.1.2066.0, 8.1.2052.0 und früher aus der jeweiligen Versionsfamilie
- ESET Server Security für Windows Server (ehemals File Security für Microsoft Windows Server) 10.0.12014.0, 9.0.12018.0, 8.0.12015.0, 7.3.12011.0 und früher aus der jeweiligen Versionsfamilie

Wie ist die Bedrohungslage auf meiner Anlage?

Auf allen Leitsystem-Rechner (Server, Clients) ist die Software von ESET installiert.

Die Schwachstelle bei der Verarbeitung von Dateivorgängen, die von der Funktion „Echtzeit-Dateisystemschutz“ des Windows-Betriebssystems ausgeführt wird, ermöglichte es einem Angreifer möglicherweise, mit der Fähigkeit, niedrigprivilegierten Code auf dem Zielsystem auszuführen, beliebige Dateien wie „NT AUTHORITY\SYSTEM“ zu löschen. ihre Privilegien ausweiten.

Wie kann ich mich dagegen schützen?

ESET hat korrigierte Builds seiner Consumer-, Business- und Server-Sicherheitsprodukte für das Windows-Betriebssystem vorbereitet und empfiehlt, auf diese zu aktualisieren oder die Upgrades in naher Zukunft zu planen.

Für Unterstützung können Sie sich kostenpflichtig an die Hotline unter 0844 11 22 11 wenden. Wenn Sie den Update-Service nutzen, entfallen die Kosten.

Update Service
Jedes System sollte regelmässig aktualisiert werden, um es gegen neu entdeckte Schwachstellen zu schützen. Gerade bei einer Firewall empfehlen wir Ihnen einen regelmässigen Software-Update, da es sich um die wichtigste Netzwerk-Sicherheits-Komponente zum Schutz ihres Netzwerkes handelt.

Mit dem Service übernimmt Rittmeyer periodisch die Kontrolle der Security, das Testen und Installieren der Software- Updates.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity