THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Matthias Deeg, Sven Freund

DEAKTIVIERUNG VON ENDPOINT PROTECTION-SOFTWARE AUF NICHT AUTORISIERTE WEISE (REVISITED)

Wie sich die passwortbasierte Authentifizierung für das Deaktivieren von Kaspersky Endpoint Security 10 for Windows und anderer Endpoint Protection-Softwareprodukte als eingeschränkter Nutzer umgehen lässt

September 2016

Wohlboldstraße 8, 72072 Tübingen, Germany

+49 (0)7071 - 40 78 56-0

info@syss.de

www.syss.de

Einleitung

Allgemein stellt Endpoint Protection-Software eine Sicherheitsmaßnahme zum Schutz von IT-Systemen wie beispielsweise Client- oder Serversystemen vor verschiedenen Bedrohungen dar. Typische Merkmale von Endpoint Protection-Software sind Antiviren- und Schadsoftwareerkennung, Kontrollmechanismen für Anwendungen und Geräte (Application/Device Control) oder spezifische Firewallfunktionalitäten.

Endpoint Protection-Software besitzt oftmals einen Passwortschutz, um den Zugriff auf eine Managementkonsole für Einstellungsänderungen oder für das Deaktivieren von Schutzfunktionen ausschließlich auf dazu berechtige Benutzer zu beschränken. Dieser Passwortschutz verringert das Risiko unautorisierter oder unbeabsichtigter Änderungen hinsichtlich der Funktionsweise der Endpoint Protection-Software und zudem ist es generell eine gute Idee administrativen Zugriff einzuschränken – besonders wenn es um Sicherheit geht (Prinzip der geringsten Berechtigungen, Principle of Least Privilege).

Um auf entsprechend geschützte Managementfunktionalität zuzugreifen und diese zu nutzen, wird üblicherweise ein Passwort benötigt (passwortbasierte Authentifizierung). In manchen Situationen kann eine solche passwortbasierte Authentifizierung für den IT-Support hilfreich sein. Aber falls sie nicht korrekt implementiert wurde, sind niederprivilegierte Angreifer oder Schadsoftware in der Lage, die Einstellungen bezüglich Schutzfunktionen zu ändern oder den Schutz vollständig auf nicht autorisierte Weise zu deaktivieren ohne das korrekte Passwort zu kennen, was die Endpoint Protection-Software im Endeffekt nutzlos macht.

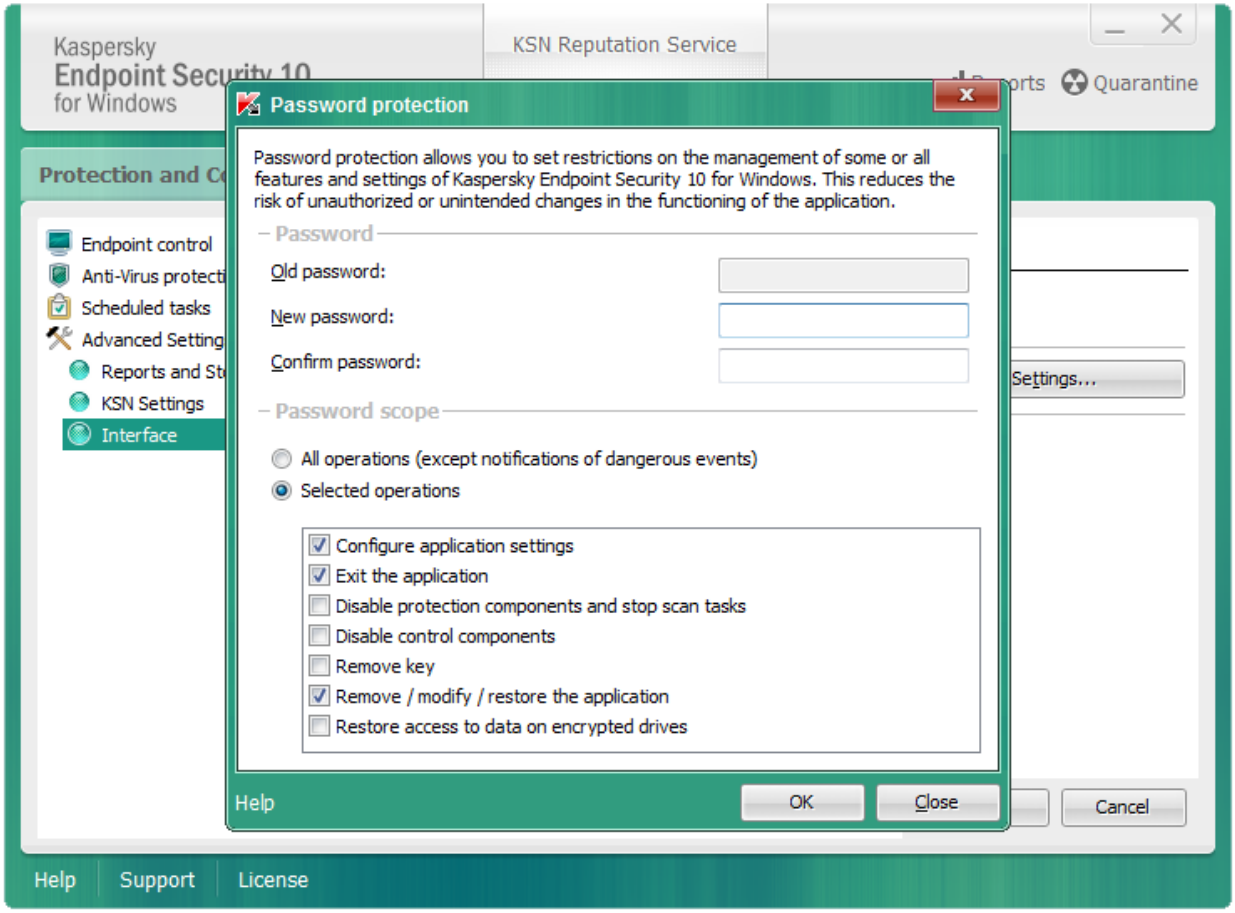


Abbildung 1: Passwortschutz von Kaspersky Endpoint Security 10

Bereits im Jahr 2012 veröffentlichte die SySS GmbH eine Fallstudie über eine Schwachstelle zum Umgehen einer Authentifizierungsmethode (Authentication Bypass) in der Endpoint Protection-Software Trend Micro OfficeScan [1]. Aber da die genannte Sicherheitslücke in moderner Endpoint Protection-Software immer noch vorhanden ist, haben wir uns dazu entschlossen, diese weniger beachtete Schwachstelle erneut ins Bewusstsein zu rufen.

In dieser Veröffentlichung wird beschrieben, wie das Verletzen sicherer Entwurfsprinzipen Authentication Bypass-Schwachstellen verursachen kann, die in aktuellen Endpoint Protection-Softwareprodukten verschiedener Hersteller im Jahr 2015 gefunden wurden. Alle behandelten Sicherheitsschwachstellen sind den Herstellern betroffener Softwareprodukte gemäß unserer Responsible Disclosure Policy [2] gemeldet worden und wurden in mehreren SySS Security Advisories [3-19] veröffentlicht sowie in einem Fachvortrag auf der IT-Sicherheitskonferenz DeepSec im November 2015 präsentiert [20].

Sicherheitsanalyse

Während eines Sicherheitstests untersuchte die SySS GmbH die Endpoint Protection-Software Kaspersky Endpoint Security 10 for Windows (KES 10), die einen Passwortschutz für Managementfunktionen anbietet, wie Abbildung 1 auf Seite 1 illustriert.

Wenn der Passwortschutz von KES 10 aktiviert ist, dann können alle geschützten Funktionen über die grafische Benutzeroberfläche (GUI) oder über das Kommandozeilenwerkzeug `avp.exe` nur mit Kenntnis des korrekten Passworts genutzt werden.

Bei der Nutzung des Kommandozeilenwerkzeugs `avp.exe` ohne Angabe des benötigten Passworts über das entsprechende Kommandozeilenargument wird eine Passworteingabe angezeigt, wie Abbildung 2 zeigt.

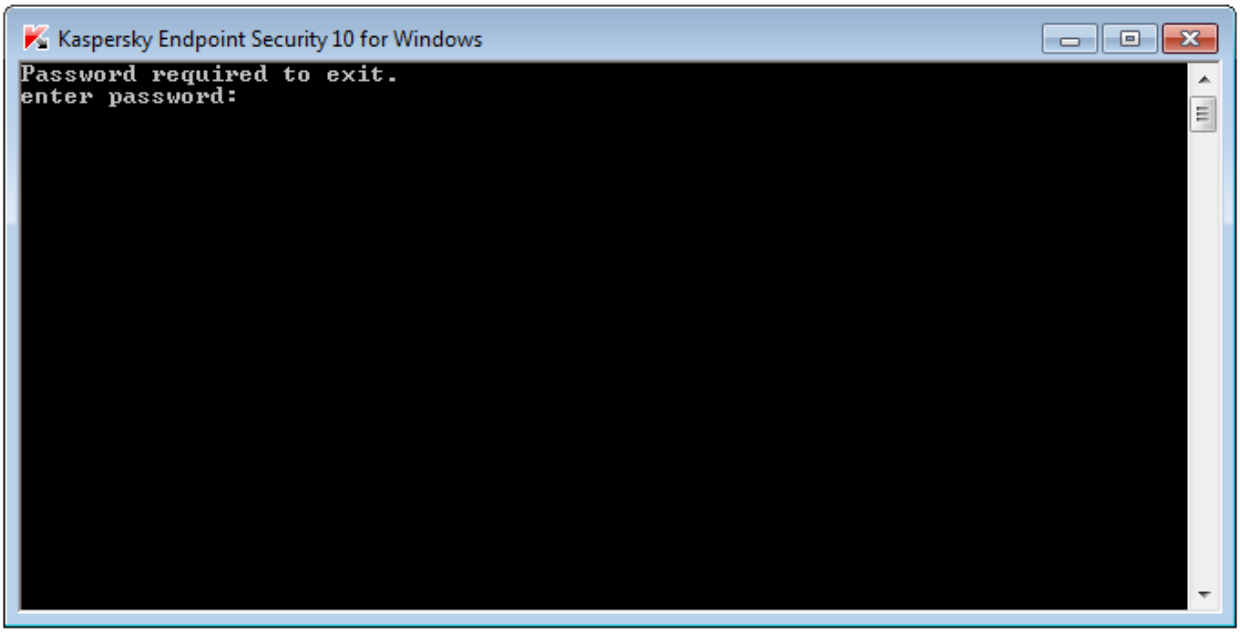


Abbildung 2: Passworteingabe des Kommandozeilenwerkzeugs `avp.exe`

Bei der Analyse der passwortbasierten Authentifizierung für die Deaktivierung von KES 10 (`EXIT`-Kommando) stellte die SySS GmbH fest, dass der Passwortvergleich innerhalb des Prozesses `avp.exe` stattfindet, der

im Kontext des aktuellen Windows-Benutzers ausgeführt wird. Bei dem Benutzer kann es sich dabei auch um einen Standardbenutzer mit eingeschränkten Benutzerberechtigungen handeln. Diese Tatsache erlaubt eine weitere Analyse und zudem eine Manipulation des Passwortvergleichs zur Laufzeit ohne administrative Berechtigungen, da jeder Benutzer in der Lage ist diejenigen Prozesse zu debuggen und zu manipulieren, die mit seinen Benutzerberechtigungen laufen.

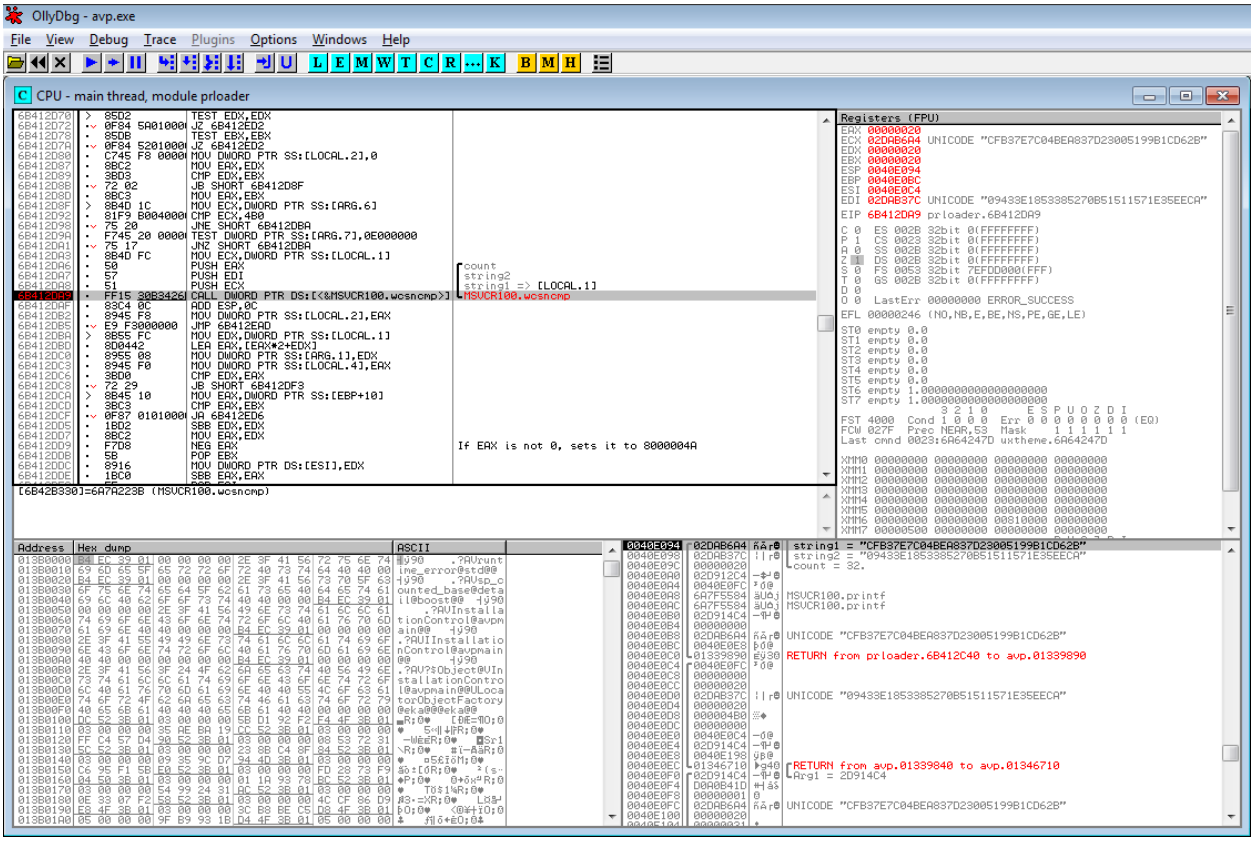


Abbildung 3: Passwortvergleich in `avp.exe` dargestellt in OllyDbg

Abbildung 3 und 4 auf Seite 3 zeigen den entsprechenden Code für den Vergleich des MD5-Hash-Werts des eingegebenen Benutzerpasswortes mit dem MD5-Hash-Wert des korrekten Passworts von KES 10 im Software-Debugger OllyDbg [21].

Um diese passwortbasierte Authentifizierung zu umgehen, muss ein Angreifer lediglich diesen Passwortvergleich modifizieren, sodass er immer erfolgreich ist, beispielsweise indem das korrekte Passwort mit sich selbst verglichen wird oder durch eine Manipulation des Programmkontrollflusses.

Die Ursache für diese Authentication Bypass-Schwachstelle ist das Verletzen sicherer Designprinzipien. Der Passwortvergleich wird innerhalb der weniger vertrauenswürdigen niedrigprivilegierten Umgebung des Prozesses `avp.exe` durchgeführt anstatt innerhalb einer vertrauenswürdigeren höherprivilegierten Umgebung eines KES 10 Dienstprozesses, auf den nicht von einem niedrigprivilegierten Prozess aus zugegriffen werden kann. Abbildung 5 auf Seite 4 illustriert dieses Sicherheitsproblem.

Wie Abbildung 6 auf Seite 5 zeigt, besteht zudem die Möglichkeit, den MD5-Hash-Wert des korrekten Passworts als niedrigprivilegierter Benutzer aus dem Speicher des Prozesses `avp.exe` zu extrahieren.

```
6B412DA3  .  8B4D FC      MOV ECX,DWORD PTR SS:[LOCAL.1]
6B412DA6  .  50           PUSH EAX                          count
6B412DA7  .  57           PUSH EDI                          string2
6B412DA8  .  51           PUSH ECX                          string1 => [LOCAL.1]
6B412DA9  .  FF15 30B3426 CALL DWORD PTR DS:[<&MSVCR100.wcsncmp>] MSVCR100.wcsncmp
6B412DAF  .  83C4 0C      ADD ESP,0C
```

Abbildung 4: Vergrößerte Darstellung des Passwortvergleichs von KES 10

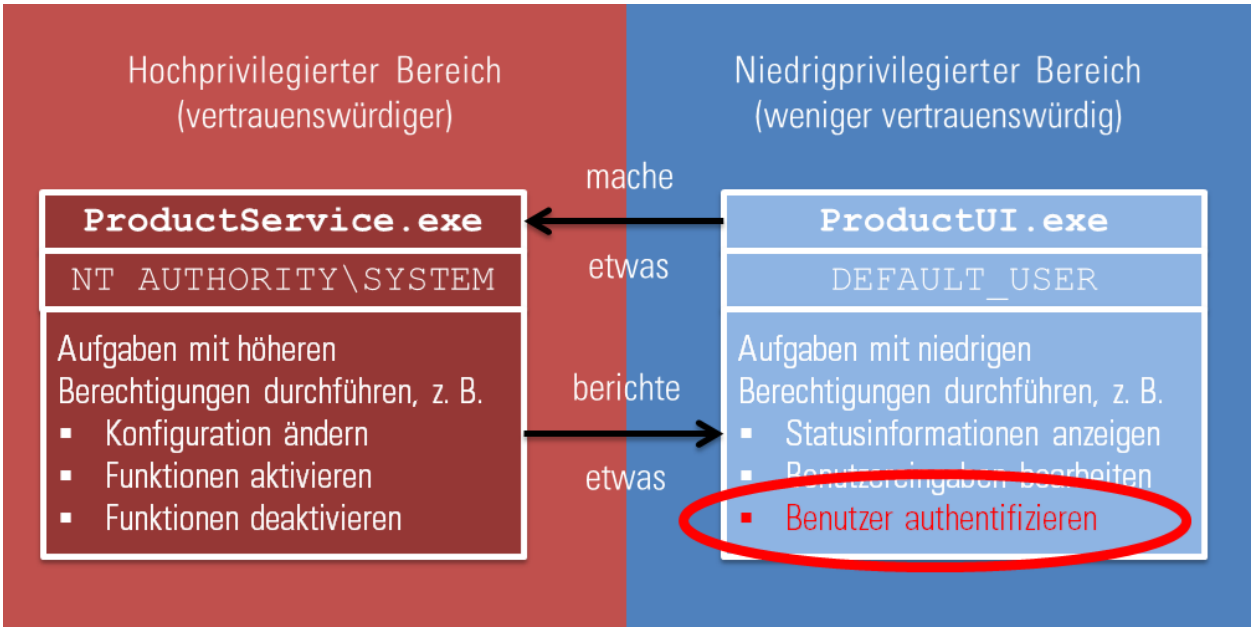


Abbildung 5: Ursache für Authentication Bypass-Schwachstelle

Im Fall von KES 10 handelt es sich bei den verwendeten MD5-Hash-Werten um sogenannte unsalted MD5-Hash-Werte unter Verwendung der Codierung UTF-16LE für das Passwort ohne terminierendes NULL-Byte. Dieser Sachverhalt wird beispielhaft anhand des Passworts `syss` in Listing 1 illustriert.

```
$ echo -en "s\x00y\x00s\x00s\x00" | md5sum
cfb37e7c04bea837d23005199b1cd62b  -
```

Listing 1: Unsalted MD5-Hash-Werte

Die Verwendung der kryptografischen Hash-Funktion MD5 ohne Nutzung eines Salt ermöglicht einem Angreifer mit Zugriff auf diese Passwortdaten die Durchführung effizienter Passwort-Rate-Angriffe mittels vorberechneter Wörterbücher, beispielsweise Rainbow Tables, um das entsprechende Klartextpasswort wiederherzustellen.

Eine weitere Möglichkeit, um als niedrigprivilegierter Benutzer auf den MD5-Hash-Wert des korrekten Passworts zuzugreifen, ist einfach das Auslesen des folgenden Windows-Registrierungsschlüssels, wie Abbildung 7 zeigt.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\
protected\KSES10\settings\OPEP
```

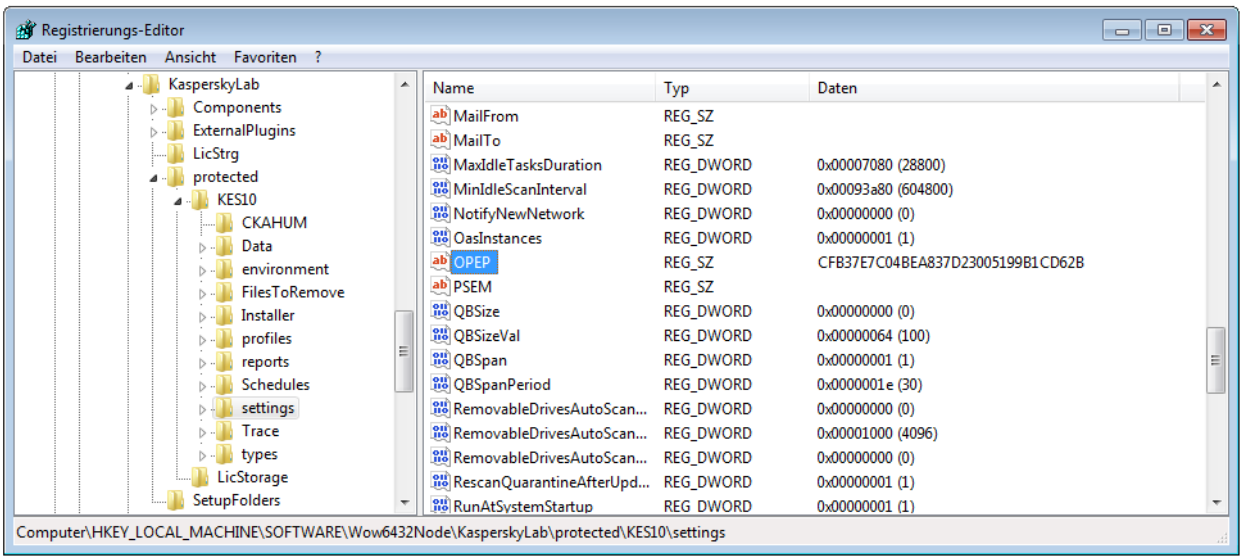


Abbildung 6: Registrierungsschlüssel mit dem MD5-Hash-Wert des korrekten Passworts

Abbildung 7: Vergrößerte Darstellung der verwendeten MD5-Passwort-Hash-Werte während der passwortbasierten Authentifizierung

Dieser Registrierungsschlüssel ist in den Standardeinstellungen für jeden Benutzer lesbar. Daher existieren zwei Wege für einen niedrigprivilegierten Benutzer oder Schadsoftware auf die unzureichend geschützten sensiblen Passwortinformationen zuzugreifen.

Betroffene Endpoint Protection-Softwareprodukte

Neben Kaspersky Endpoint Security 10 for Windows untersuchte die SySS GmbH auch weitere Endpoint Protection-Softwareprodukte auf Authentication Bypass-Schwachstellen hin.

In Tabelle 1 werden alle Endpoint Protection-Softwareprodukte aufgeführt, die ebenfalls anfällig für Authentication Bypass-Angriffe waren und die sensible Passwortinformationen nur unzureichend schützten.

Proof-of-Concept

Die SySS GmbH entwickelte verschiedene Proof-of-Concept-Software-Tools, um die betroffenen Endpoint Protection-Softwareprodukte auf unautorisierte Weise zu deaktivieren.

Ein Beispiel für ein solches Proof-of-Concept-Software-Tool ist UnloadKES. Dieses Software-Tool ist ein einfacher Loader mit Patch-Funktionalität, der wie folgt arbeitet:

Produktname	Getestete Softwareversion
BullGuard Antivirus	15.0.297
BullGuard Premium Protection	15.0.297
BullGuard Internet Security	15.0.297
Kaspersky Anti-Virus (KAV)	6.0.4.1611, 15.0.1.415
Kaspersky Endpoint Security for Windows (KES)	8.1.0.1042, 10.2.1.23, 10.2.2.10535
Kaspersky Internet Security (KIS)	15.0.2.361
Kaspersky Small Office Security (KSOS)	13.0.4.233
Kaspersky Total Security (KTS)	15.0.1.415
Panda Antivirus Pro 2015	15.1.0
Panda Global Protection 2015	15.1.0
Panda Gold Protection 2015	15.1.0
Panda Internet Security 2015	15.0.1

Tabelle 1: Endpoint Protection-Softwareprodukte

1. Auffinden der ausführbaren Datei `avp.exe`
2. Erzeugen einer neuen Instanz des Prozesses `avp.exe` unter Verwendung eines Kommandozeilenarguments für die Nutzung der `EXIT`-Funktion
3. Manipulation der passwortbasierten Authentifizierung des neu erzeugten Prozesses `avp.exe`, sodass jedes Passwort als korrekt angesehen wird
4. Stoppen des Debuggings des Prozesses und Fortsetzen der Programmausführung

Die Ausgabe von UnloadKES in Listing 2 zeigt beispielhaft die erfolgreiche Deaktivierung von KES 10. Die entwickelten Software-Tools UnloadPanda und UnloadBullguard für getestete Endpoint Protection-Softwareprodukte der Hersteller Panda Security und Bullguard Ltd. konnten nicht nur die Endpoint Protection-Software auf nicht autorisierte Weise deaktivieren, sondern auch das korrekte Klartextpasswort auslesen, wie die beiden Listings 3 auf Seite 8 und 4 auf Seite 9 illustrieren.

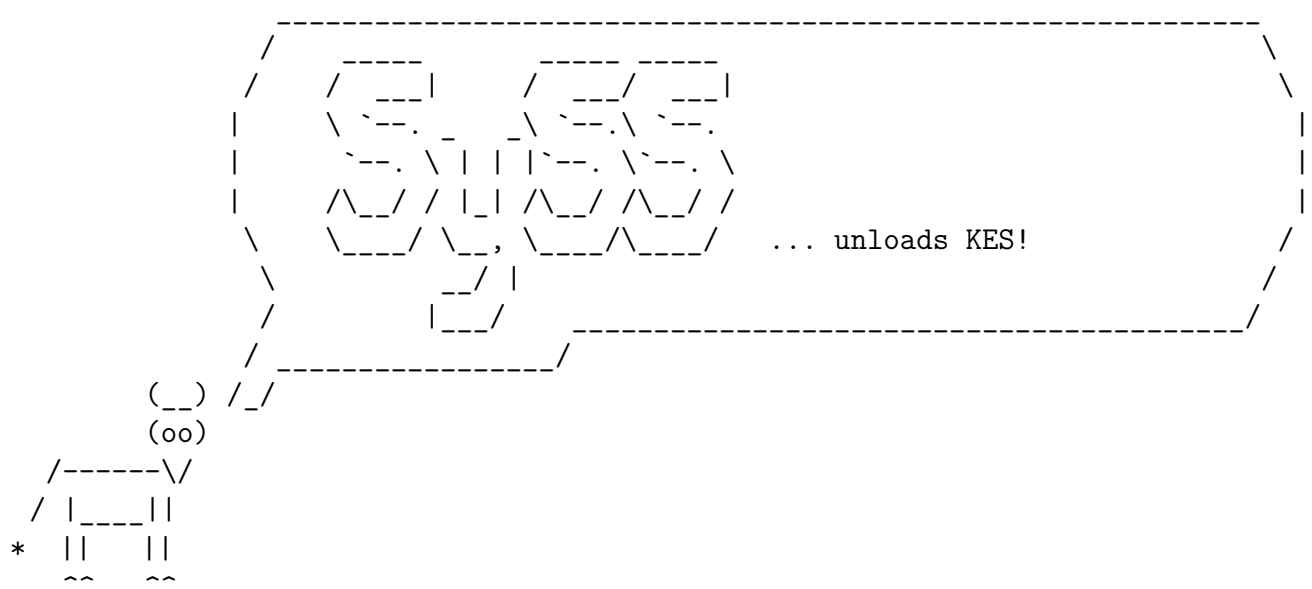
Fazit und Empfehlung

Unsere Forschungsergebnisse zeigen, dass sich auch im Jahr 2015 manche Endpoint Protection-Softwareprodukte immer noch auf unautorisierte Weise durch niedrigprivilegierte Benutzer oder Schadsoftware aufgrund von Authentication Bypass-Schwachstellen deaktivieren ließen.

Die Ursache hierfür war das Verletzen sicherer Designprinzipien. Sicherheitsrelevante Aufgaben, wie beispielsweise Authentifizierung, wurden nicht innerhalb einer vertrauenswürdigen höherprivilegierten Umgebung durchgeführt, auf die nicht von niedrigprivilegierten Benutzern oder Schadsoftware zugegriffen werden kann, sondern innerhalb einer weniger vertrauenswürdigen niedrigprivilegierten Umgebung die Manipulationen mit unerwünschten Konsequenzen erlaubt, wie beispielsweise das Umgehen von Authentifizierungsmethoden.

Sicherheitsschwachstellen wie Authentication Bypass-Schwachstellen, die lokale Angriffsszenarien in nicht netzwerkbasierten Softwarefunktionen betreffen, und der unzureichende Schutz von Passwortinformationen sollten nicht vernachlässigt werden, da sie in manchen Angriffsszenarien für einen Angreifer den Unterschied zwischen einer erfolgreichen Systemkompromittierung und einem „Show Stopper“ machen. Um diese Sicherheitsschwachstellen zu verhindern, empfiehlt die SySS GmbH Folgendes:

```
>UnloadKES.exe
```

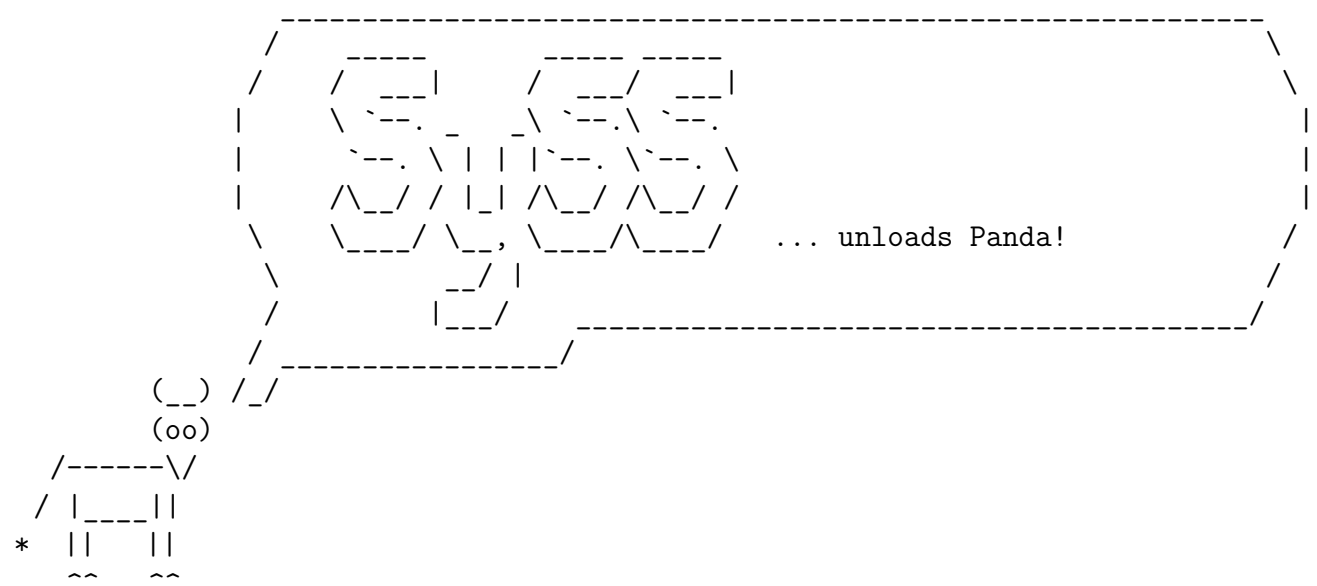



```
SySS Unload KES v1.0 by Sven Freund & Matthias Deeg - SySS GmbH (c) 2015
[+] Found location of the executable file avp.exe
[+] Created new instance of the Kaspersky Endpoint Security process avp.exe
[+] The Kaspersky Endpoint Security process was patched successfully.
    Kaspersky Endpoint Security will now exit without a password.
```

Listing 2: Erfolgreiche Deaktivierung von KES 10 mittels UnloadKES

- Immer Vertrauen in der Informationssicherheit berücksichtigen:
  - Vertrauensbereiche (Trust Domains)
  - Vertrauensgrenzen (Trust Boundaries)
  - Vertrauensbeziehungen (Trust Relationships)
- Sicherheitsrelevante Aufgaben in einer vertrauenswürdigeren Umgebung durchführen
- Nicht zu viele Annahmen treffen
- Passwortinformationen vernünftig schützen:
  - Zugang zu Passwortinformationen auf Benutzer beschränken, die diese Informationen wirlich benötigen
  - Kryptografisch sichere, standardisierte Algorithmen mit einer passenden Konfiguration verwenden, beispielsweise PBKDF2
- Dem Prinzip der niedrigsten Berechtigungen folgen (Principle of Least Privilege)

```
>UnloadPanda.exe
```




```
SySS Unload Panda Protection v1.0 by Matthias Deeg - SySS GmbH (c) 2015
[+] The Panda process was patched successfully.
    Now you can unload the Panda protection with an arbitrary password.
    After entering an arbitrary password, the correct one will be shown.
[+] The correct password is: s3cret1!
```

Listing 3: Erfolgreicher Deaktivierung der Endpoint Protection-Software von Panda und Auslesen des korrekten Passworts mittels UnloadPanda

Referenzen

[1] Deeg, Matthias/Schreiber, Sebastian: Case Study: Deactivating Endpoint Protection Software in an Unauthorized Manner, https://www.syss.de/fileadmin/dokumente/Publikationen/2012/SySS_2012_Deeg_Case_Study_-_Deactivating_Endpoint_Protection_Software_in_an_Unauthorized_Manner.pdf

[2] SySS Responsible Disclosure Policy, https://www.syss.de/fileadmin/dokumente/Publikationen/2016/SySS_Responsible_Disclosure_Policy.pdf

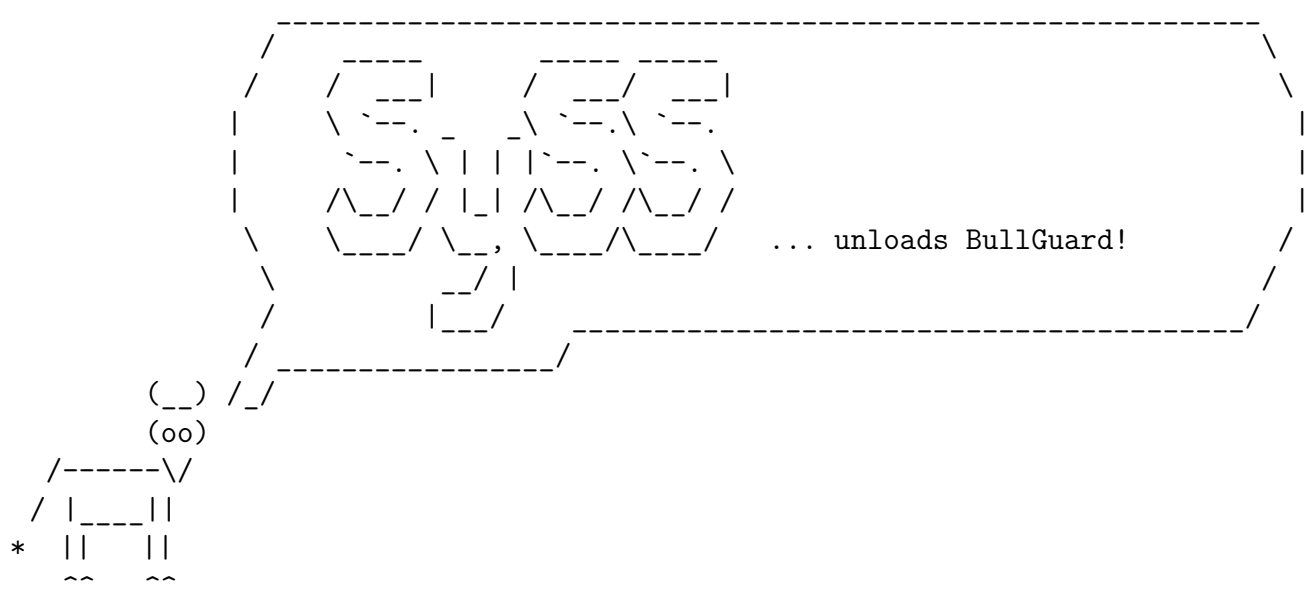
[3] Freund, Sven/Deeg, Matthias: SySS Security Advisory SYSS-2015-001, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-001.txt

[4] Freund, Sven/Deeg, Matthias: SySS Security Advisory SYSS-2015-002, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-002.txt

[5] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-003, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-003.txt

[6] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-004, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-004.txt

```
>UnloadBullguard.exe
```




```
SySS Unload BullGuard v1.0 by Matthias Deeg - SySS GmbH (c) 2015
[+] Found location of the executable file BullGuard.exe
[+] Created new instance of the process BullGuard.exe
[+] The BullGuard process was patched successfully.
    Now you can unload the BullGuard protection with an arbitrary password.
    After entering an arbitrary password, the correct one will be shown.
[+] The correct password is: S3cret1!
```

Listing 4: Erfolgreiche Deaktivierung der Endpoint Protection-Software von BullGuard und Auslesen des korrekten Passworts mittels UnloadBullguard

[7] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-005, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-005.txt

[8] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-006, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-006.txt

[9] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-007, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-007.txt

[10] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-008, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-008.txt

[11] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-009, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-009.txt

[12] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-010, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-010.txt

[13] Deeg, Matthias: SySS Security Advisory SYSS-2015-012, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-012.txt

[14] Deeg, Matthias: SySS Security Advisory SYSS-2015-013, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-013.txt

[15] Deeg, Matthias: SySS Security Advisory SYSS-2015-014, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-014.txt

[16] Deeg, Matthias: SySS Security Advisory SYSS-2015-015, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-015.txt

[17] Deeg, Matthias: SySS Security Advisory SYSS-2015-017, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-017.txt

[18] Deeg, Matthias: SySS Security Advisory SYSS-2015-017, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-018.txt

[19] Deeg, Matthias: SySS Security Advisory SYSS-2015-017, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-019.txt

[20] Deeg, Matthias: Deactivating Endpoint Protection Software in an Unauthorized Manner, DeepSec 2015, https://www.syss.de/fileadmin/dokumente/Publikationen/2015/Deactivating_Endpoint_Protection_Software_in_an_Unauthorized_Manner_-_DeepSec_2015.pdf, https://vimeo.com/152394408

[21] OllyDbg, http://www.ollydbg.de/

Wohlboldstraße 8, 72072 Tübingen, Germany

+49 (0)7071 - 40 78 56-0

info@syss.de

www.syss.de

THE PENTEST EXPERTS

SySS GmbH Wohlboldstraße 8 72072 Tübingen +49 (0)7071 - 40 78 56-0 info@syss.de

WWW.SYSS.DE