SySS
THE PENTEST EXPERTS.

IT SECURITY KNOW-HOW

Matthias Deeg, Sven Freund

DEACTIVATING ENDPOINT PROTECTION SOFTWARE IN AN UNAUTHORIZED MANNER (REVISITED)

How to Bypass the Password-Based Authentication for Unloading Kaspersky Endpoint Security 10 for Windows and other Endpoint Protection Software Products as a Limited User

September 2016

Wohlboldstraße 8, 72072 Tübingen, Germany

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

info@syss.de

www.syss.de

Introduction

In general, endpoint protection software is a security control measure to protect IT systems, for example client or server systems, from different threats. Typical features of endpoint protection software are anti-virus and malware detection, application and device control mechanisms, or specific firewall functionalities.

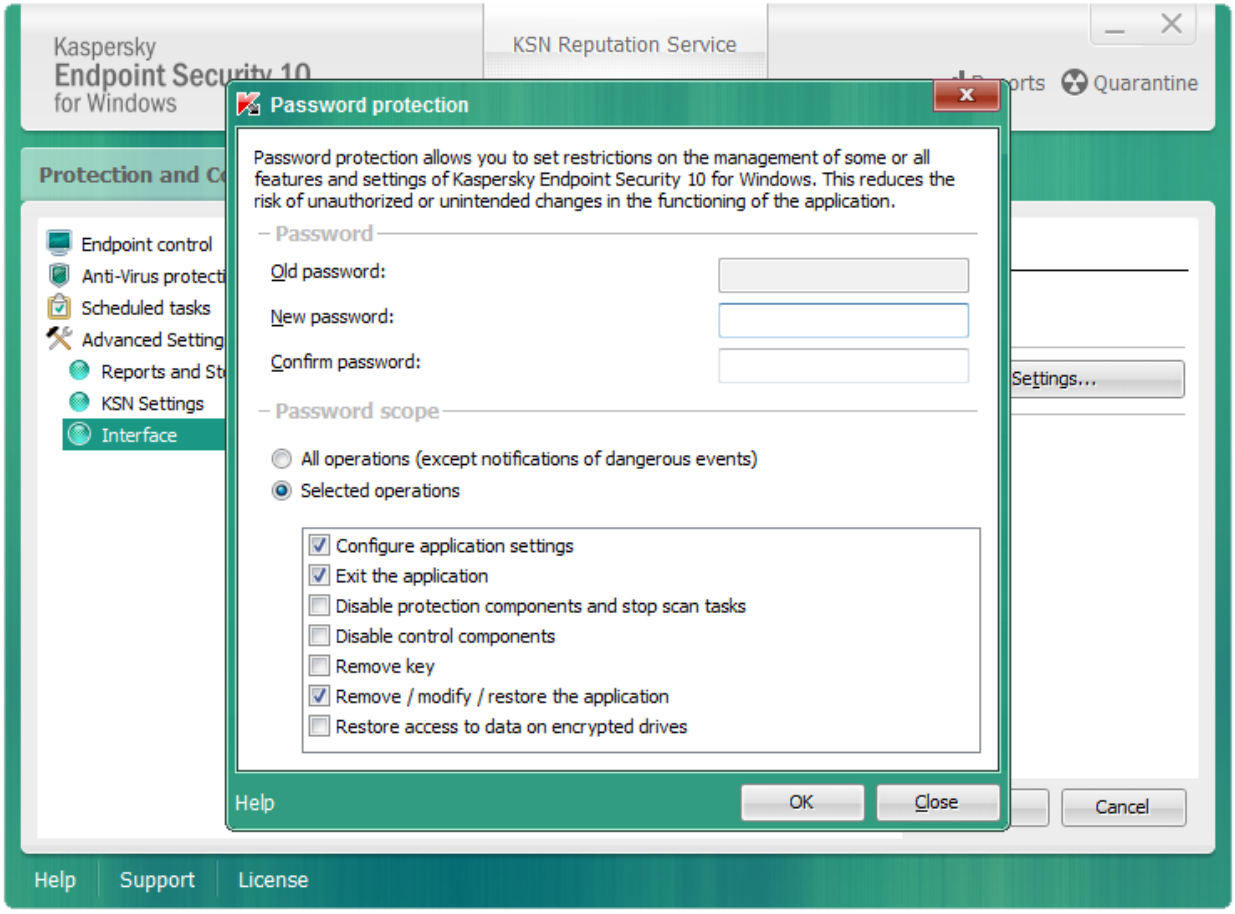


Figure 1: Password protection of Kaspersky Endpoint Security 10

Endpoint protection software often is password protected in order to restrict access to a management console for changing settings or deactivating protection features to authorized users only. This protection reduces the risk of unauthorized or unintended changes in the functioning of the software, and restricting administrative access is generally a good idea – especially when it comes to security (principle of least privilege).

In order to access and use a protected management functionality, a password usually is required (password-based authentication). In some situations, this feature can be useful for IT support. But if the password-based authentication is not implemented properly, low-privileged attackers or malware are able to change the protection settings or to deactivate the protection entirely in an unauthorized manner without having to know the correct password rendering the endpoint protection software useless.

In 2012, SySS GmbH already published a case study about an authentication bypass vulnerability affecting the endpoint protection software Trend Micro OfficeScan [1]. But as this type of security vulnerability is still present in modern endpoint protection software, we decided to raise awareness for this less regarded security issue again.

In this paper, it will be shown how the violation of secure design principles can cause authentication bypass vulnerabilities that were found in current endpoint protection software products of different vendors in 2015. All the discussed security vulnerabilities have been reported to the manufacturers of the affected software products according to our responsible disclosure policy [2] and were publicly disclosed in several SySS security advisories [3-19], and in a talk at the IT security conference DeepSec in November 2015 [20].

Security analysis

During a security assessment, SySS GmbH analyzed the endpoint protection software Kaspersky Endpoint Security 10 for Windows that offers a password protection for management features, as Figure 1 on Page 1 illustrates.

If the password protection of KES 10 is enabled, all protected operations can only be performed either via the GUI or the command line tool `avp.exe` if the correct password is known.

When using the command line tool `avp.exe` and not setting the required password via the command line argument, a password prompt is shown, as Figure 2 illustrates.

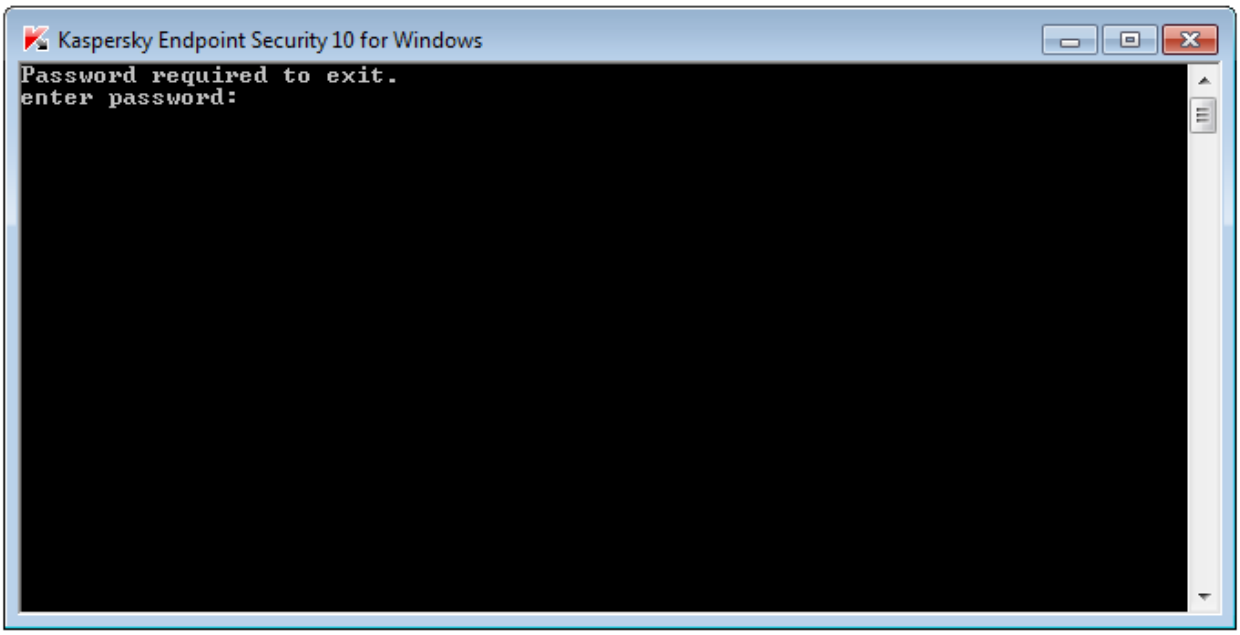


Figure 2: Password prompt of command line tool `avp.exe`

By analyzing the password-based authentication for unloading KES 10 (`EXIT` command), SySS GmbH found out that the password comparison is done within the process `avp.exe`, which runs or can be run in the context of the current Windows user who can also be a standard, limited user. This fact allows a further analysis and additionally the manipulation of the password comparison during runtime without administrative privileges, as every user is able to debug and manipulate the processes running with his user privileges.

Figure 3 and 4 on Page 3 show the corresponding code for comparing the MD5 hash of the password entered by the user with the MD5 hash of the correct password within the software debugger OllyDbg [21].

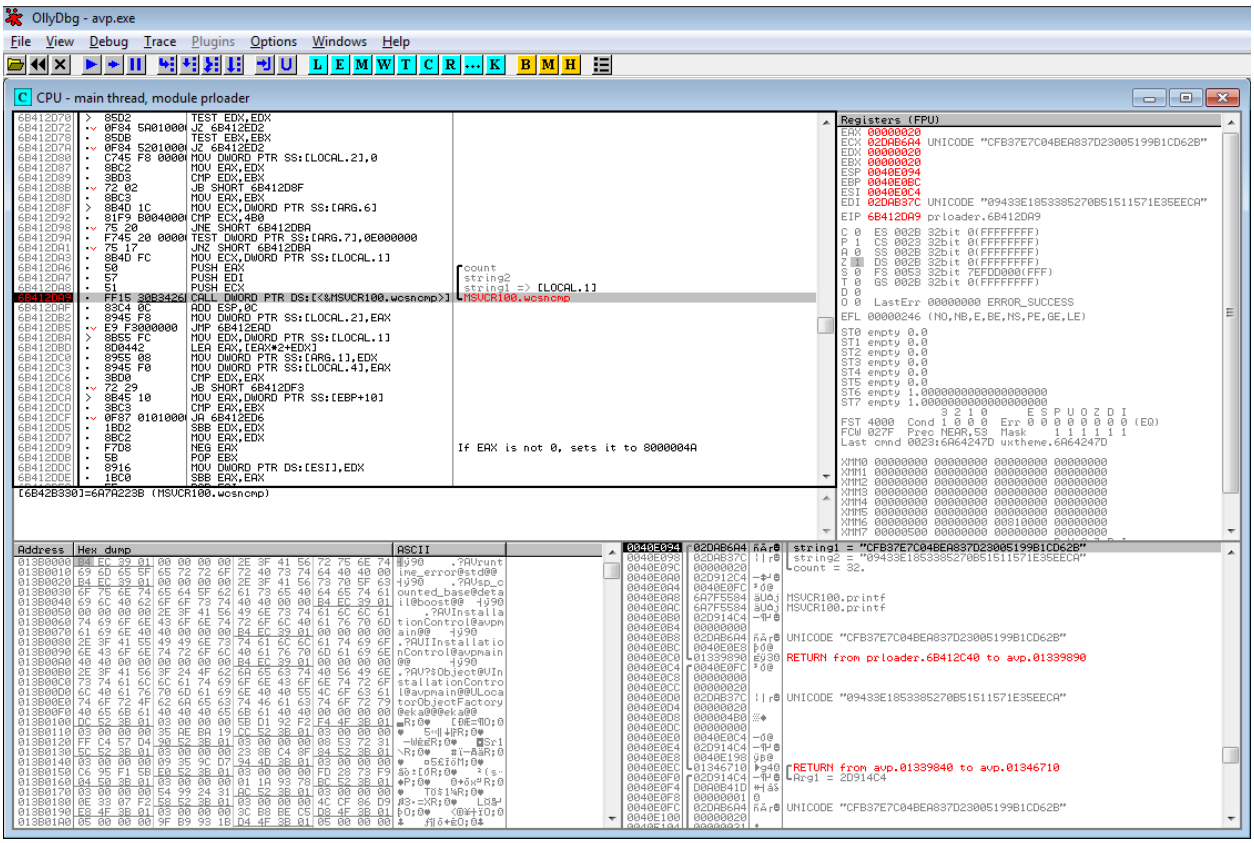


Figure 3: Password comparison within `avp.exe` shown in OllyDbg

In order to bypass this password-based authentication, an attacker only has to patch this password comparison, so that it always returns true, for example by comparing the correct password with itself or by modifying the program control flow.

The cause for this authentication bypass vulnerability is the violation of secure design principles. The password comparison is done within the less trustworthy low-privileged domain of the process `avp.exe` instead of a more trustworthy high-privileged domain of a KES 10 service process that is not accessible by a low-privileged user. Figure 5 on Page 4 illustrates this security issue.

In case of KES 10, the used MD5 hashes actually are unsalted MD5 hashes using UTF-16LE encoding of the password without the terminating null byte. This is exemplarily illustrated in Listing 1 on Page 4 for the password `syss`.

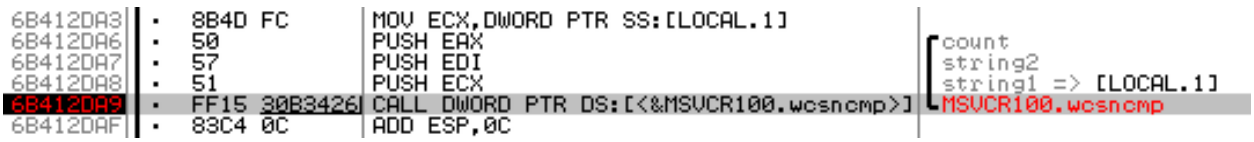


Figure 4: Close-up of password comparison in KES 10

As Figure 6 on Page 5 illustrates, it is also possible to extract the MD5 hash of the correct password as a low-privileged user from the memory of the process `avp.exe`.

The use of the cryptographic one-way hash function MD5 without using a salt allows an attacker with access to this data to perform efficient password-guessing attacks using pre-computed dictionaries, for instance rainbow tables, in order to recover the corresponding cleartext password.

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

Listing 1: Unsalted MD5 hashes

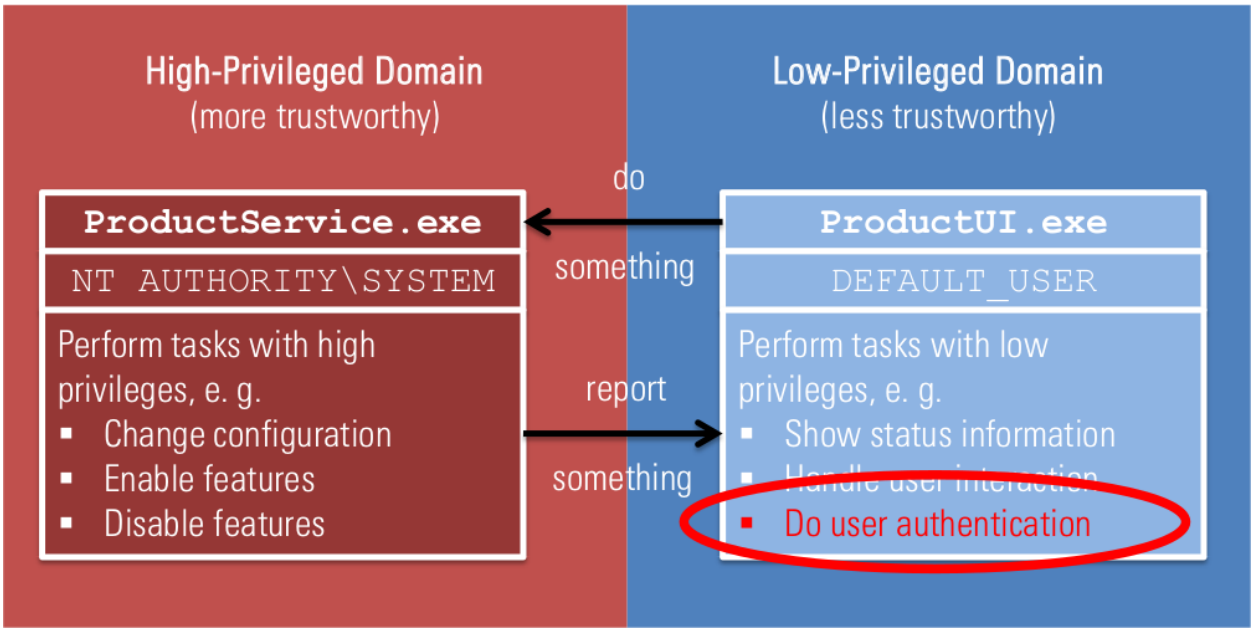


Figure 5: Cause of authentication bypass vulnerability

Another way to access the MD5 hash of the correct password as a low-privileged user is to simply read the following Windows registry key, as Figure 6 illustrates.

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

This registry key is by default readable by every user. Thus, there are two ways for a low-privileged user or malware to access the insufficiently protected sensitive password information.

Figure 6: Close-up of MD5 password hashes used during the password-based authentication

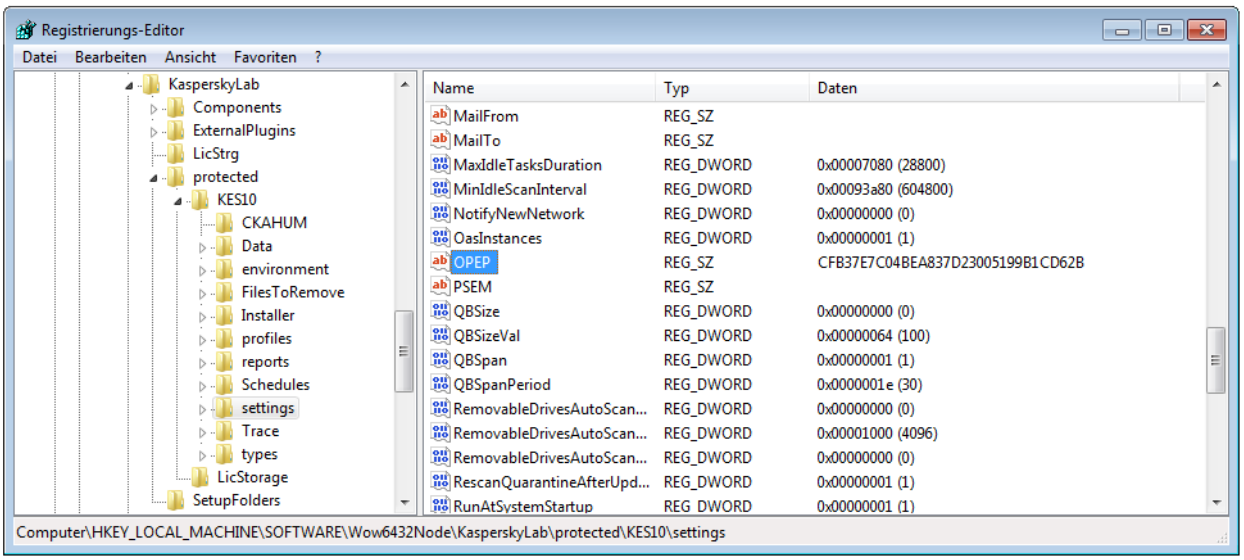


Figure 7: Registry key with the MD5 hash of the correct password

Affected endpoint protection software products

Besides Kaspersky Endpoint Security 10 for Windows, SySS GmbH also analyzed other endpoint protection software products for authentication bypass vulnerabilities.

Table 1 lists all affected endpoint protection software products that were also vulnerable to authentication bypass attacks and insufficiently protected sensitive password information.

Product name	Tested software version
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

Table 1: Endpoint protection software products

Proof-of-concept

SySS GmbH developed different proof-of-concept software tools for deactivating affected endpoint protection software products in an unauthorized manner.

One example of such a proof-of-concept software tool is UnloadKES. This software tool is a simple loader with patching functionality and works as follows:

1. Find the executable file `avp.exe`
2. Create a new instance of the process `avp.exe` with a command line argument to trigger the `EXIT` function
3. Patch the password-based authentication of the newly created process `avp.exe` so that any password is considered correct
4. Stop debugging the process and continue its execution

The UnloadKES output shown in Listing 2 on Page 7 exemplarily shows a successful deactivation of Kaspersky Endpoint Security for Windows. Concerning the tested endpoint protection software products by the manufactures Panda Security and BullGuard Ltd., the developed proof-of-concept software tools UnloadPanda and UnloadBullguard could not only deactivate the endpoint protection software in an unauthorized manner, but also extract the correct cleartext password, as the Listings 3 (Page 8) and 4 (Page 9) illustrate.

Conclusion and recommendation

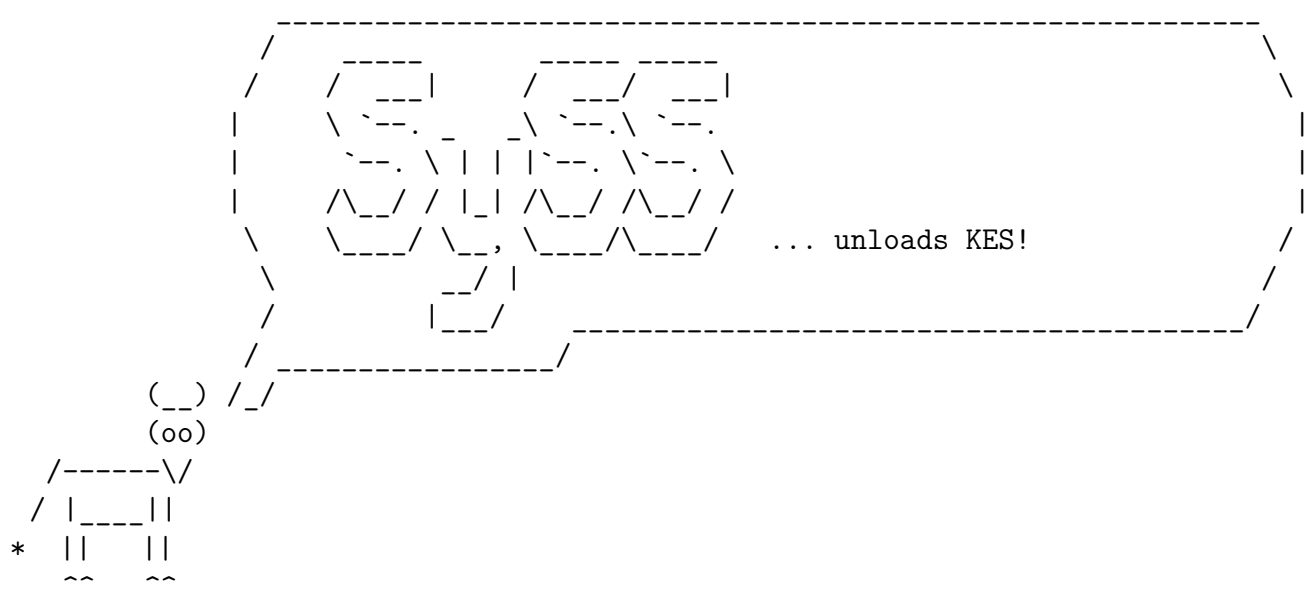
Our security research shows that in 2015 some endpoint protection software products could still be deactivated in an unauthorized manner by low-privileged users or malware due to authentication bypass vulnerabilities. The cause for this was the violation of secure design principles. Security-related tasks like authentication were not performed within a trustworthy high-privileged domain that is not accessible to low-privileged users or malware, but within a less trustworthy low-privileged domain that allows for manipulations with unwanted consequences like authentication bypass.

Security issues like authentication bypass vulnerabilities concerning local attack scenarios in non-networked software features and insufficient protection of user credentials should not be neglected, as in some scenarios they can make the difference between a successful system compromise and a show stopper for an attacker.

In order to prevent these security issues, SySS GmbH recommends the following:

- Always consider trust in IT security:
  - Trust domains
  - Trust boundaries
  - Trust relationships
- Perform security-related tasks in a more trustworthy environment
- Do not make too much assumptions
- Properly protect password information:
  - Restrict access to password information to required users only
  - Use cryptographically secure standard algorithms with a suitable configuration, e. g. PBKDF2
- Follow the principle of least privilege

```
>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: Successful deactivation of KES 10 via UnloadKES

References

[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

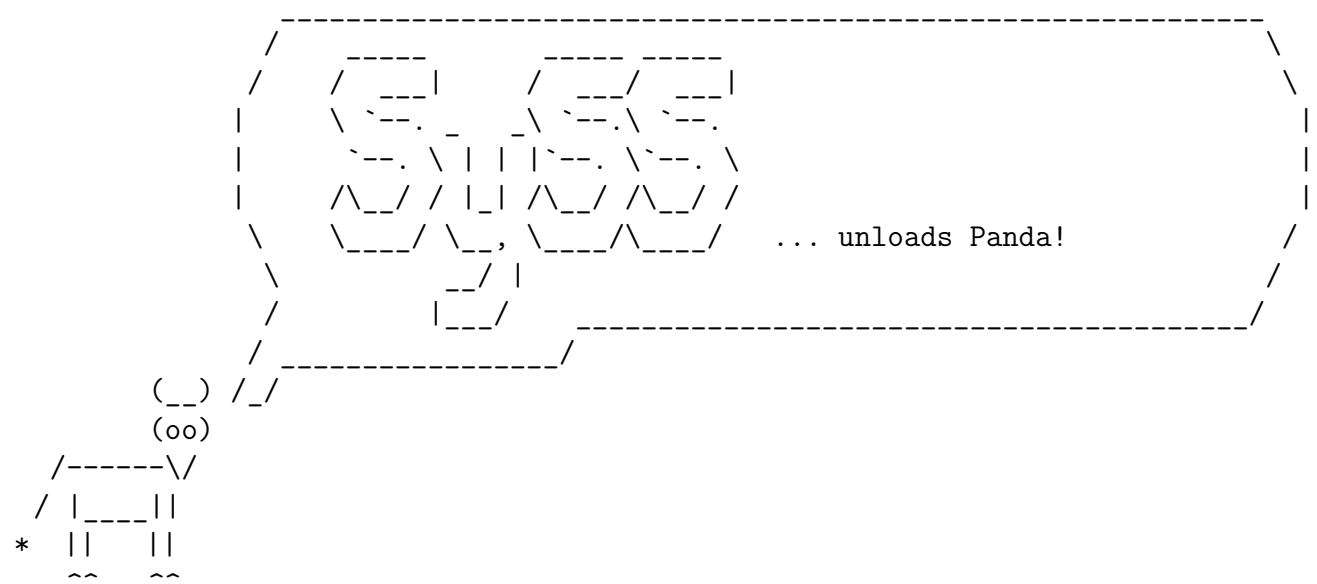
[4] Freund, Sven/Deeg, Matthias: SySS Security Advisory SYSS-2015-002, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-002.txt

[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

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

```
>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: Successful deactivation of a Panda endpoint security software and extracting the correct password via UnloadPanda

[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

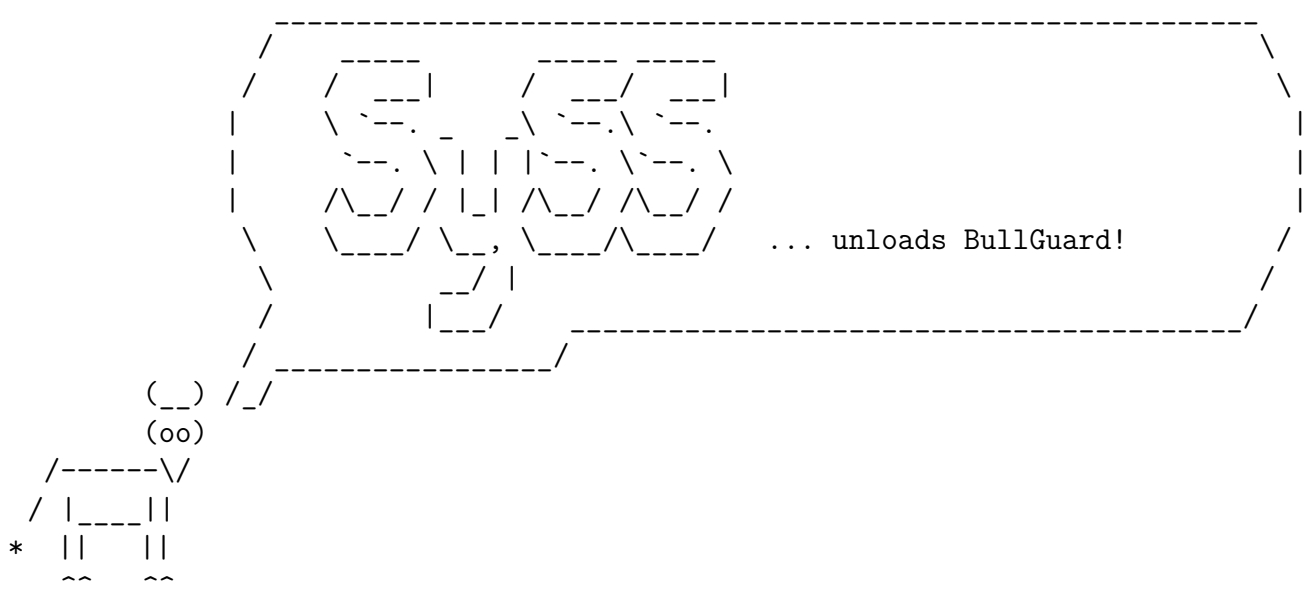
[12] Deeg, Matthias/Freund, Sven: SySS Security Advisory SYSS-2015-010, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2015-010.txt

[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

```
>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: Successful deactivation of a BullGuard endpoint security software and extracting the correct password via UnloadBullguard

[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/

THE PENTEST EXPERTS

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

WWW.SYSS.DE