

Feature: Scan-Notizen

Inhalt

- [Notiz anlegen und in PDF-Bericht übernehmen](#)
- [Notiz verallgemeinern](#)
- [Notizen-Management](#)

Einleitung

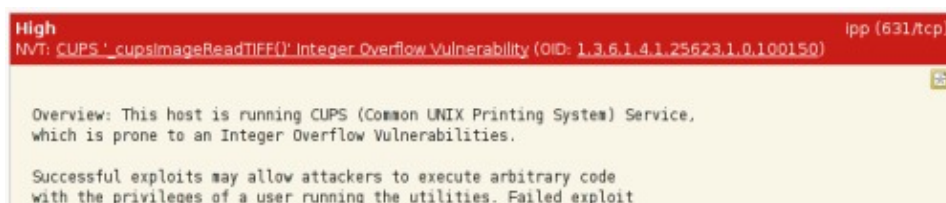
Teil der anspruchsvollen Funktionalität des Schwachstellen-Managements ist die umfassende Unterstützung von Notizen.

Notizen können zu jedem Einzelergebnis eines Scan-Reports angelegt und ja nach Wunsch in die (PDF-)Berichte aufgenommen werden.

Darüber hinaus können Notizen verallgemeinert werden, z.B. auf alle Zielsysteme mit dem gleichen Problem: Hat man einmal eine Notiz zu einem Scan-Resultat angelegt und verallgemeinert, so wird die Notiz in allen bestehenden und allen zukünftigen Berichten an der passenden Stelle eingefügt.

Notiz anlegen und in PDF-Bericht übernehmen

Für jedes einzelne Resultat kann über das -Icon eine neue Notiz angelegt werden.



Der grundlegende und unveränderbare Bezug einer Notiz ist der Network Vulnerability Test (NVT). Beim Anlegen der Notiz ist zunächst ein direkter Bezug auf das Zielsystem, Port, Schweregrad und Task voreingestellt.

New Note ?

Hosts	<input type="radio"/> Any <input checked="" type="radio"/> 127.0.0.1
Port	<input type="radio"/> Any <input checked="" type="radio"/> lpp (631/tcp)
Threat	<input type="radio"/> Any <input checked="" type="radio"/> High
Task	<input type="radio"/> Any <input checked="" type="radio"/> Standard scan
Result	<input type="radio"/> Any <input checked="" type="radio"/> ac05507f-0247-4159-b7cf-45ae46702925
Text	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p style="color: red; margin: 0;">Why is CUPS running on this host anyway? Better remove the service entirely.</p> </div>

Associated Result

High
lpp (631/tcp)

NVT: CUPS_cupsImageReadTIFF() Integer Overflow Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100150)

Overview: This host is running CUPS (Common UNIX Printing System) Service, which is prone to an Integer Overflow Vulnerabilities.

Mit "Create Note" wird die Notiz angelegt und das Scan-Resultat um diese Notiz ergänzt.

Jede Notiz kann direkt vom Report-Browser aus gelöscht (✖), bearbeitet (🔧) oder mit allen Details betrachtet werden (🔍).

Da einige Resultate sehr lang sein können, zeigt das 📄-Icon an, dass eine Notiz unten zu finden ist. Klickt man das Icon an springt man direkt zu der Notiz.

High
lpp (631/tcp)

NVT: CUPS_cupsImageReadTIFF() Integer Overflow Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100150)

Overview: This host is running CUPS (Common UNIX Printing System) Service, which is prone to an Integer Overflow Vulnerabilities.

Successful exploits may allow attackers to execute arbitrary code with the privileges of a user running the utilities. Failed exploit attempts likely cause denial-of-service conditions.

Affected Software/OS:
CUPS versions prior to 1.3.10

Solution:
Updates are available. Please see <http://www.cups.org/software.php> for more information.

References:
<http://www.securityfocus.com/bid/34571>
<http://www.cups.org/str.php?l3031>

Risk factor: High
CVE : CVE-2009-0163
BID : 34571

Note

Why is CUPS running on this host anyway?
Better remove the service entirely.

Last modified: Fri Mar 19 12:15:54 2010.

Der Filter für die Ergebnisse erlaubt das Ein- und Ausschalten der Darstellung der Notizen über den Schalter "Show notes".

Result Filtering

Results 1 - 8 of 8 This report as: PDF

Sorting: [port_ascending](#) | [port_descending](#) | [threat_ascending](#) | [threat_descending](#)

Show notes

Text phrase:

Threat: High Medium Low Log

Dieser Schalter bestimmt auch für die herunterladbaren PDF-Berichte ob die Notizen angehängt werden.

2 RESULTS PER HOST 3

... continued from previous page ...

http://www.cups.org/str.php?L3031

Risk factor: High
CVE : CVE-2009-0183
EID : 34571

OID of test routine: 1.3.6.1.4.1.25623.1.0.100150

Note
Why is CUPS running on this host anyway?
Better remove the service entirely.

Last modified: Fri Mar 19 12:15:54 2010

Notiz verallgemeinern

Jede Notiz kann so verallgemeinert werden, dass sie wie in diesem Beispiel sehr weitgehend für sämtliche Zielsysteme, Ports oder Tasks gültig ist.

New Note ?

Hosts Any 127.0.0.1

Port Any ipp (631/tcp)

Threat Any High

Task Any Standard scan

Result Any ac05507f-0247-4159-b7cf-45ae46702925

Text

We do have a security-fixed package in our internal package repository. See security page of our intranet.

Associated Result

High ipp (631/tcp)
NVT: CUPS' cupsImageReadTIFF()' Integer Overflow Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100150)

Overview: This host is running CUPS (Common UNIX Printing System) Service, which is prone to an Integer Overflow Vulnerabilities.

Ab diesem Moment wird sie bei der Report-Ansicht immer angezeigt wenn der Bezug, hier das NVT wenn es Schweregrad "High" meldet, hergestellt werden kann.

Das gilt für alle bereits vorher erstellten Scan-Reports und für alle zukünftigen. So lange bis die Notiz wieder gelöscht wird.

Risk factor: High
CVE : CVE-2009-0163
BID : 34571

Note

We do have a security-fixed package in our internal package repository. See security page of our intranet.
Last modified: Fri Mar 19 12:28:44 2010.

Note

Why is CUPS running on this host anyway?
Better remove the service entirely.
Last modified: Fri Mar 19 12:15:54 2010.

Der Übersicht unseres Beispiel-Task kann man nun entnehmen, dass zwei Notizen einen Bezug herstellen.

Task Summary

Name: Standard scan
Config: Full and fast
Escalator:
Schedule: (Next due: over)
Target: Localhost
Status: Stopped
Reports: 1 (Finished: 0)

Reports for 'Standard scan'

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Fri Mar 19 11:46:48 2010 Stopped	High	3	5	21	18	PDF Download	

Notes on Results of 'Standard scan'

NVT	Text	Actions
CUPS '_cupsimageReadTIFF()' Intege...	We do have a security-fixed package in o...	
CUPS '_cupsimageReadTIFF()' Intege...	Why is CUPS running on this host anyway?...	

Notizen-Management

Die Verwaltung aller angelegten Notizen ist Teil des Scan-Management.

Navigation

- Scan Management
 - Tasks
 - New Task
 - Notes
 - Performance

Notes

NVT	Text	Actions
CUPS '_cupsimageReadTIFF()' Intege...	We do have a security-fixed package in o...	
CUPS '_cupsimageReadTIFF()' Intege...	Why is CUPS running on this host anyway?...	

Über die Details lassen sich Bezug und Inhalt einsehen.

Note Details ?

NVT Name: [CUPS '_cupsimageReadTIFF\(\)' Integer Overflow Vulnerability](#) [Back to Notes](#)

NVT OID: 1.3.6.1.4.1.25623.1.0.100150
 Created: Fri Mar 19 12:28:44 2010
 Last Modified: Fri Mar 19 12:28:44 2010

Application

Hosts: Any
 Port: Any
 Threat: High
 Task: Any
 Result: Any

Appearance

Note

We do have a security-fixed package in our internal package repository. See security page of our intranet.
 Last modified: Fri Mar 19 12:28:44 2010.

Es ist ein direkter Sprung zu den Details des entsprechenden NVTs möglich. Die NVT-Details listen sämtliche auf das jeweilige NVT bezogenen Notizen auf und erlauben zudem eine direkte Bearbeitung.

NVT Details ?

Name: CUPS '_cupsimageReadTIFF()' Integer Overflow Vulnerability

Summary: Check for the version of CUPS service
 Family: Denial of Service
 OID: 1.3.6.1.4.1.25623.1.0.100150
 CVE: CVE-2009-0163
 Bugtraq ID: 34571
 Other references:

Description

Overview: This host is running CUPS (Common UNIX Printing System) Service, which is prone to an Integer Overflow Vulnerabilities.

Successful exploits may allow attackers to execute arbitrary code with the privileges of a user running the utilities. Failed exploit attempts likely cause denial-of-service conditions.

Affected Software/OS:
 CUPS versions prior to 1.3.10

Solution:
 Updates are available. Please see <http://www.cups.org/software.php> for more information.

References:
<http://www.securityfocus.com/bid/34571>
<http://www.cups.org/str.php?L3031>


Risk factor: High




Notes

Text	Actions
We do have a security-fixed package in o...	
Why is CUPS running on this host anyway?...	

Notizen die derzeit für kein einziges Scan-Resultat des Benutzers Anwendung finden werden als Waise (engl. Orphan) gekennzeichnet.

Der Task dieses Beispiels wurde komplett gelöscht. Die eine Notiz hatte direkten Bezug während die andere als vom Task unabhängig eingestellt wurde.

Notes 

NVT	Text	Actions
CUPS '_cupsimageReadTIFF()' Intege...	We do have a security-fixed package in o...	  
CUPS '_cupsimageReadTIFF()' Intege...	Orphan Why is CUPS running on this host anyway?...	