SECURITY DAYS

ESET VULNERABILITY & PATCH MANAGEMENT

NOVÁ VRSTVA OCHRANY OD ESETU POMÔŽE VYRIEŠIŤ ZRANITEĽNOSTI VO FIREMNÝCH SIEŤACH

Ján Baláž, Igor Hula

Digital Security
Progress. Protected.

&

SME KONFERENCIE

Agenda

1. Úvod do problematiky a štatistiky
2. Rozšírená ponuka ESET produktov
3. Ukážka riešenia, ktoré pripravujeme
4. Priestor na diskusiu

Zraniteľnosť?

Zraniteľnosť *je slabina, ktorú môžu útočníci zneužiť na získanie neoprávneného prístupu do počítačového systému. Po zneužití zraniteľnosti môže kybernetický útok spustiť škodlivý kód, nainštalovať malvér alebo odcudziť citlivé údaje.*

CVE*, skratka pre Common Vulnerabilities and Exposures, je zoznam verejne zverejnených chýb v počítačovej bezpečnosti. Keď niekto odkazuje na CVE, myslí tým bezpečnostnú chybu, ktorej bolo pridelené ID číslo CVE.*

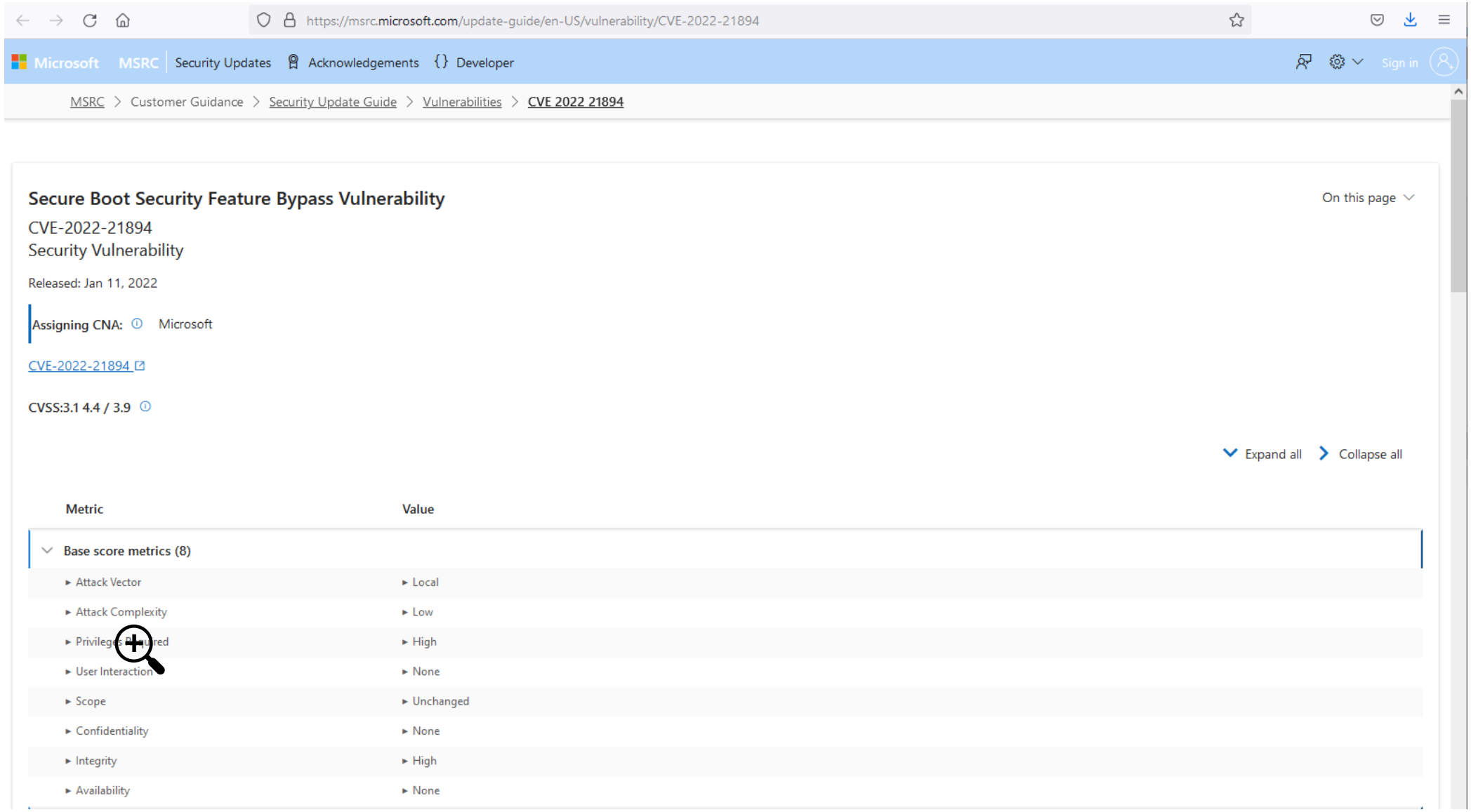
welivesecurity.com by ESET

Share

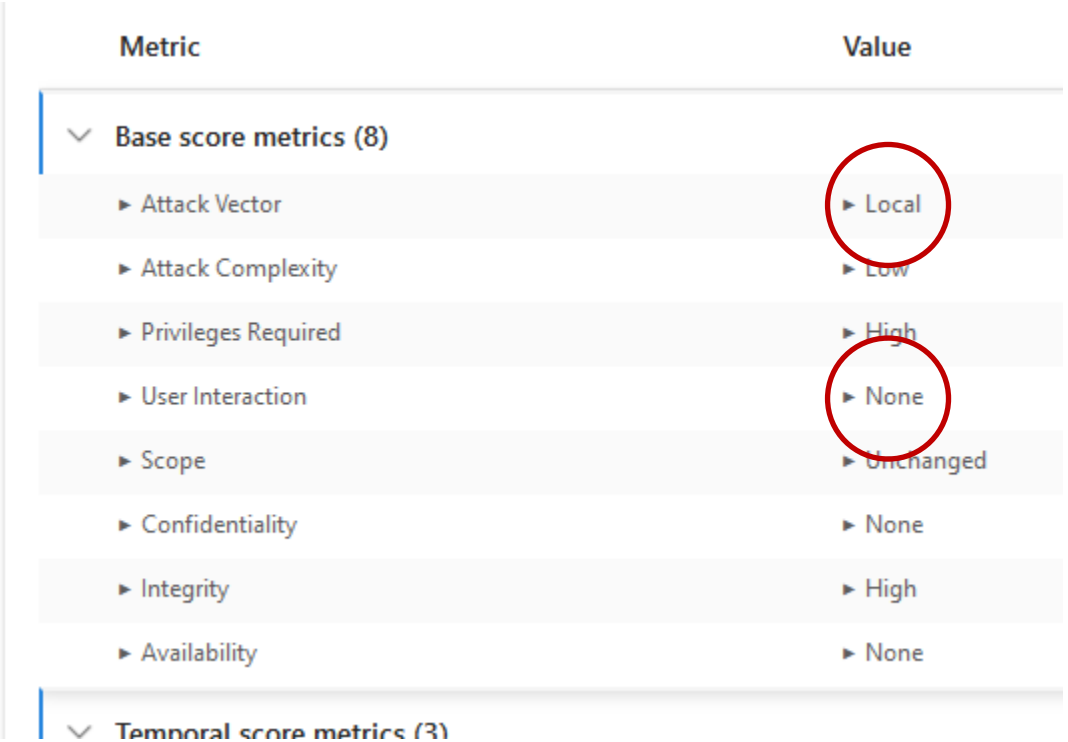
The number of UEFI vulnerabilities discovered in recent years and the failures in patching them or revoking vulnerable binaries within a reasonable time window hasn't gone unnoticed by threat actors. As a result, the first publicly known UEFI bootkit bypassing the essential platform security feature – UEFI Secure Boot – is now a reality. In this blogpost we present the first public analysis of this UEFI bootkit, which is capable of running on even fully-up-to-date Windows 11 systems with UEFI Secure Boot enabled. Functionality of the bootkit and its individual features leads us to believe that we are dealing with a bootkit known as **BlackLotus**, the UEFI bootkit being sold on hacking forums for $5,000 since at least October 2022.

UEFI bootkits are very powerful threats, having full control over the OS boot process and thus capable of disabling various OS security mechanisms and deploying their own kernel-mode or user-mode payloads in early OS startup stages. This allows them to operate very stealthily and with high privileges. So far, only a few have been discovered in the wild and publicly described (e.g., multiple malicious EFI samples we discovered in 2020, or

Microsoft Security Response Center & CVE-2022-21894



MSRC – detail z metriky



Metric	Value
Base score metrics (8)	
▸ Attack Vector	▸ Local
▸ Attack Complexity	▸ Low
▸ Privileges Required	▸ High
▸ User Interaction	▸ None
▸ Scope	▸ Unchanged
▸ Confidentiality	▸ None
▸ Integrity	▸ High
▸ Availability	▸ None
Temporal score metrics (3)	

6 pilierov manažmentu zraniteľností v podaní ESET-u

1. Úplná integrácia s konzolou ESET PROTECT Cloud (EPC)
2. Prémiová funkcionalita s vlastnou licenciou
3. Určená pre všetky dôležité platformy
4. Lokalizácia podľa štandardov EPC
5. Komponent endpoint-u, bez inštalácie a údržby
6. Praktická distribúcia záplat a hotfix-ov ako súčasť riešenia

Aktuálny prieskum IDC

The State of Cybersecurity Maturity in Vulnerability Management Among U.S. Organizations, April 2023

- 82% organizácii aktívne využíva systémy na riadenie zraniteľností, 41% z nich raz za mesiac alebo menej
- 74% organizácií kontroluje menej ako 85% firemných zariadení

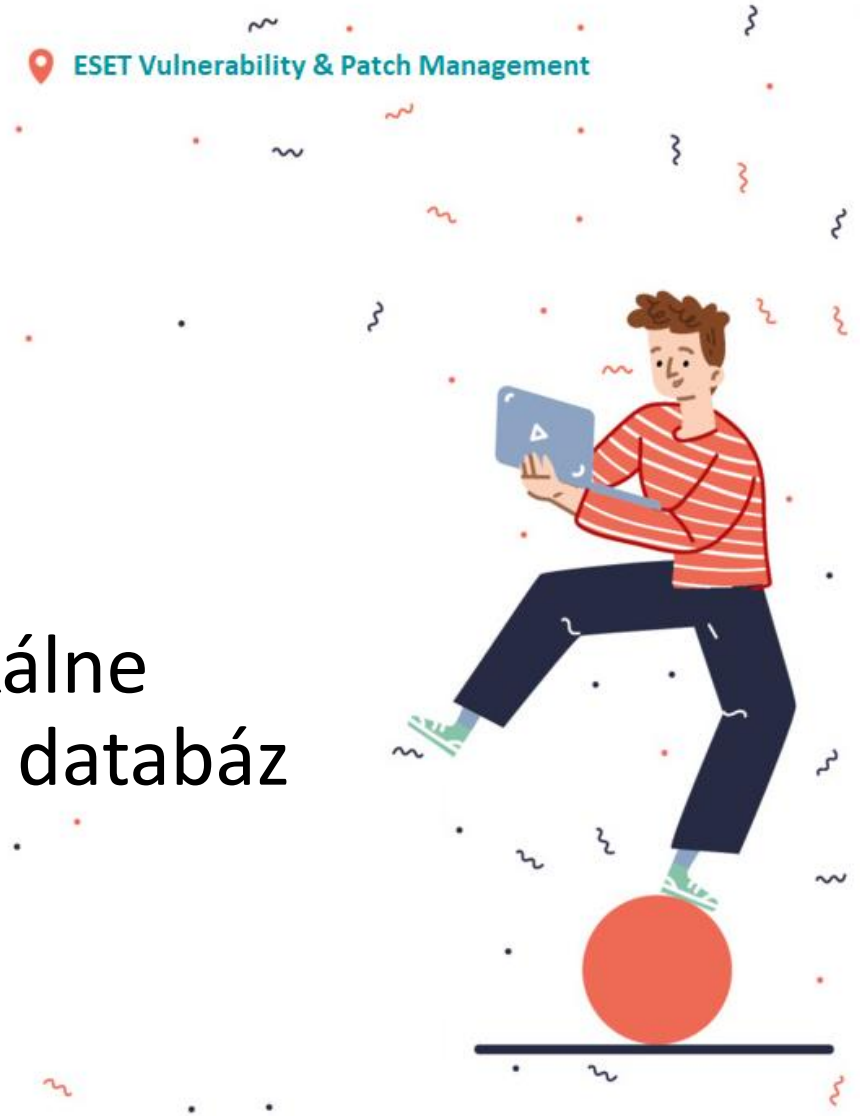
Na zamyslenie

„I still fervently believe that the only way to make software secure, reliable, and fast is to make it small. Fight Features.“

Andrew S. Tanenbaum

Umenie rovnováhy a výhody súčasnej architektúry

- **Zameranie na firemné siete**
  pomer cena/výkon, intuitívnosť a ovládanie, škálovateľnosť
  - **Bez vzdialenej telemetrie**
    žiadne profilovanie klienta, lokálne vyhodnocovanie a aktualizácia databáz

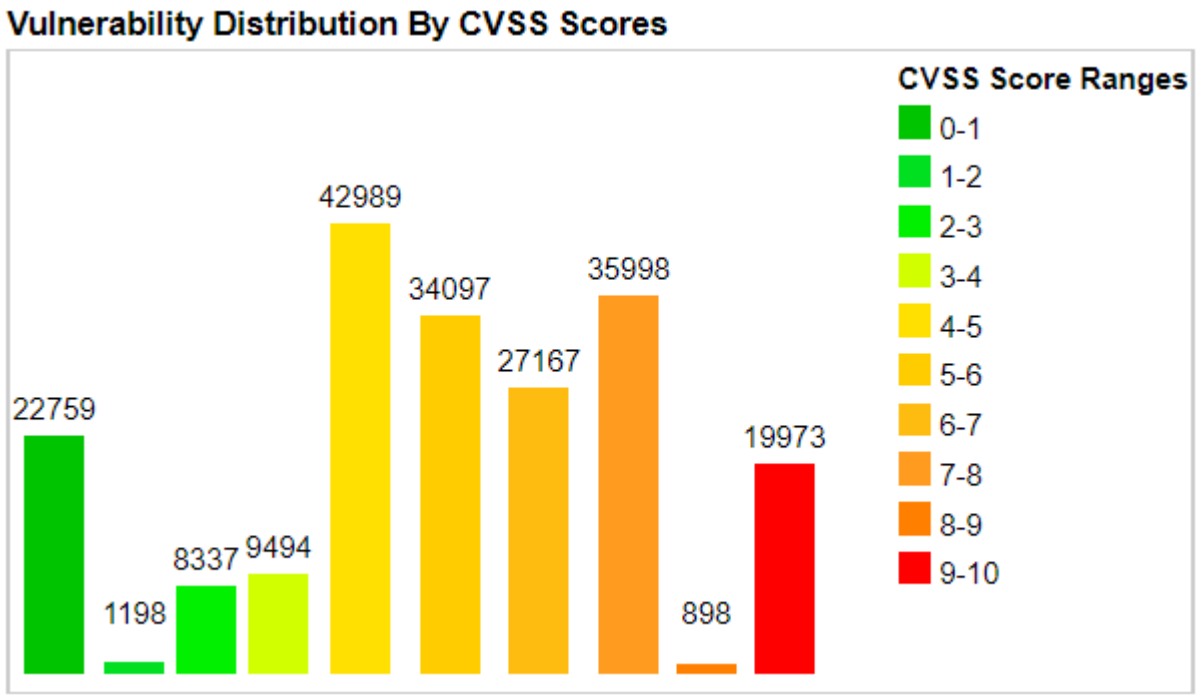


Výhody súčasnej architektúry - pokračovanie

- **Patch management pod kontrolou**
  antimalvérová vrstva preveruje záplaty a inštalátory dodávateľov softvéru
- **Jednoduchosť riešenia**
  manuálny a automatický režim
- **Nekompromisný dôraz na výkon**
  bez dodatočného agenta, konzoly, inštalácie a údržby

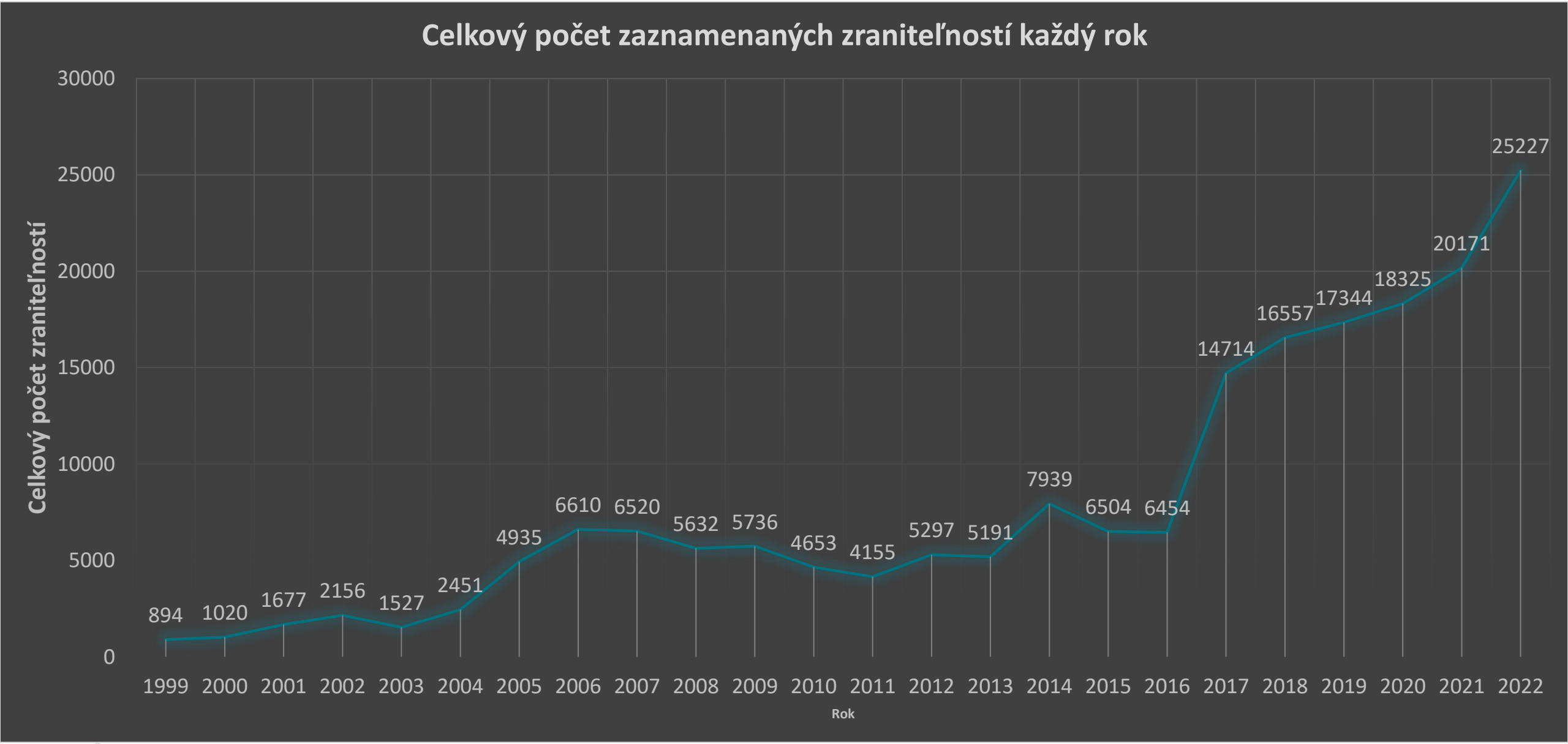
Zaujímavé štatistiky (1)

- Viac ako 75 % aplikácií má aspoň jednu známu chybu
- 75 % útokov v roku 2020 využívalo zraniteľnosti, ktoré boli najmenej dva roky staré
- Takmer 10 % všetkých zraniteľností je vysokej závažnosti



Sources: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/ ; https://www.cvedetails.com/cvss-score-distribution.php

Zaujímavé štatistiky (2)



Source: https://www.cvedetails.com/browse-by-date.php

Rozšírenie ponuky pre rok 2023 (V&PM)

		ESET PROTECT Essential	ESET PROTECT Entry	ESET PROTECT Advanced	ESET PROTECT Complete	ESET PROTECT Enterprise	ESET PROTECT Elite	ESET PROTECT MDR
Standard offering	ESET PROTECT Platform	●	●	●	●	●	●	●
	Modern Endpoint Protection	◐	●	●	●	●	●	●
	Server Security	●	●	●	●	●	●	●
	Advanced Threat Defense (ESET LiveGuard)			●	●	●	●	●
	Full Disk Encryption			●	●	●	●	●
	Mail Security				●		●	●
	Cloud App Protection				●		●	●
	Detection & Response					●	●	●
Optional offering	SharePoint Security	◐	◐	◐	◐	◐	◐	◐
	Endpoint Encryption	◐	◐	◐	◐	◐	◐	◐
New Additions 2023	Multi-Factor Authentication*	◐	◐	◐	◐	◐	●	●
New Additions 2023	Vulnerability and Patch Management				●		●	●
Services	Standard Support	●	●	●	●	●	●	●
	Premium Support Advanced	◐	◐	◐	◐	◐	◐	●
	Deployment and Upgrade	◐	◐	◐	◐	◐	◐	●
	MDR Ultimate							●
	ESET Threat Intelligence	◐	◐	◐	◐	◐	◐	◐

● Included
◐ Optional
* ESA Cloud to be available H2/2023

SECURITY DAYS

Čo pripravujeme v našom riešení

WORK IN PROGRESS

& SME KONFERENCIE

Plánované funkcionality / Roadmap

EPC 4.5 + Endpoint 10.1

- Centrálny manažment zraniteľností a záplat (nie lokálne)
- Odhaľovanie zraniteľností v bežnom softvéri
- Odhaľovanie zraniteľností v OS
- Závažnosť a kategorizácia zraniteľností
- Výnimky v evidovaných zraniteľnostiach
- Exportovanie reportov zo zraniteľností a riadenia rizík
- Odklad reštartu počítača a voľba užívateľa

EPC 5.X + Endpoint 11.X

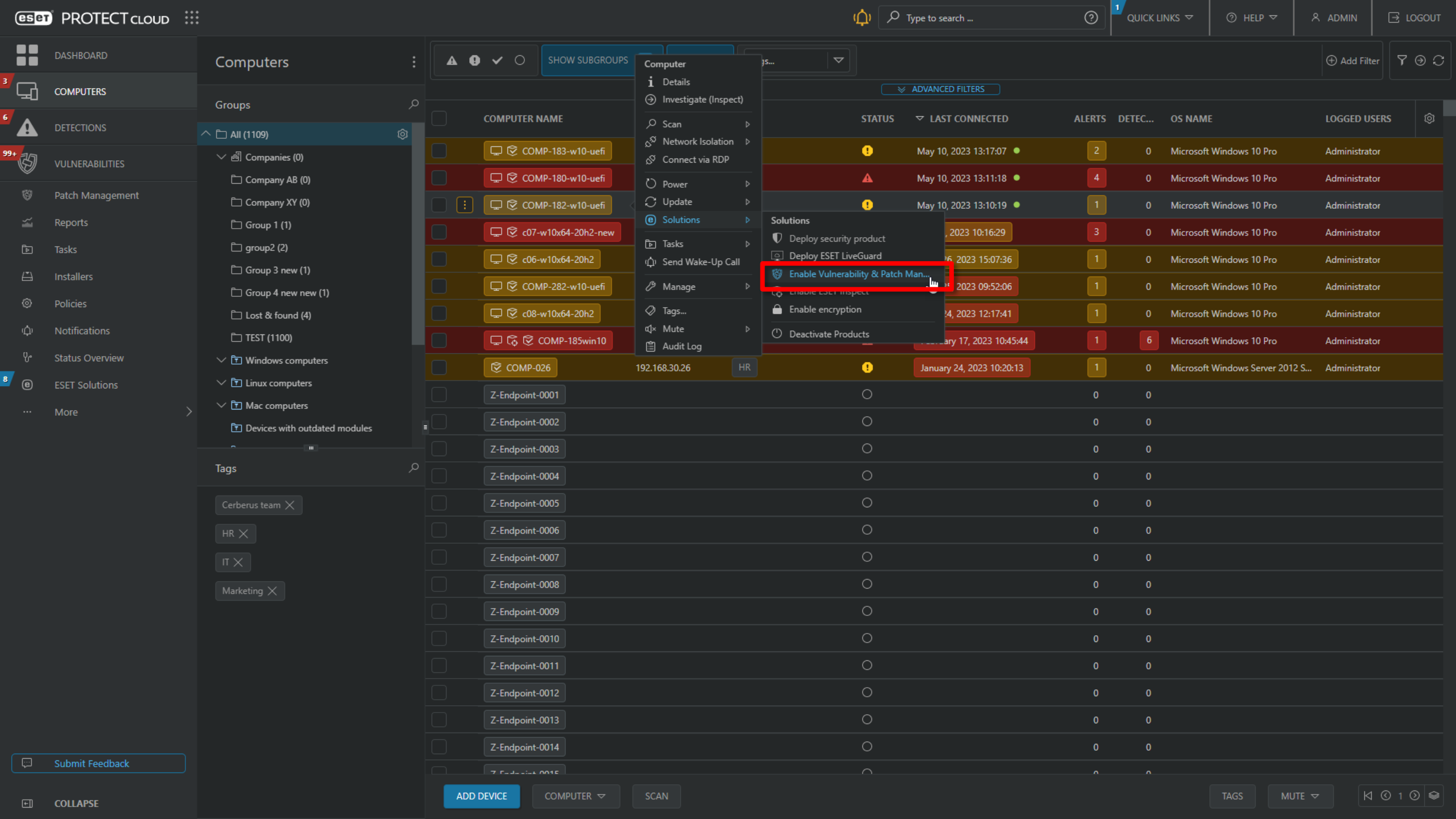
- Dashboard pre zraniteľnosti
- Časový vývoj počtu zraniteľností
- Microsoft KB referencie
- Rozširovanie pokrytia platforiem:
  - Windows Servers
  - Linux
  - macOS

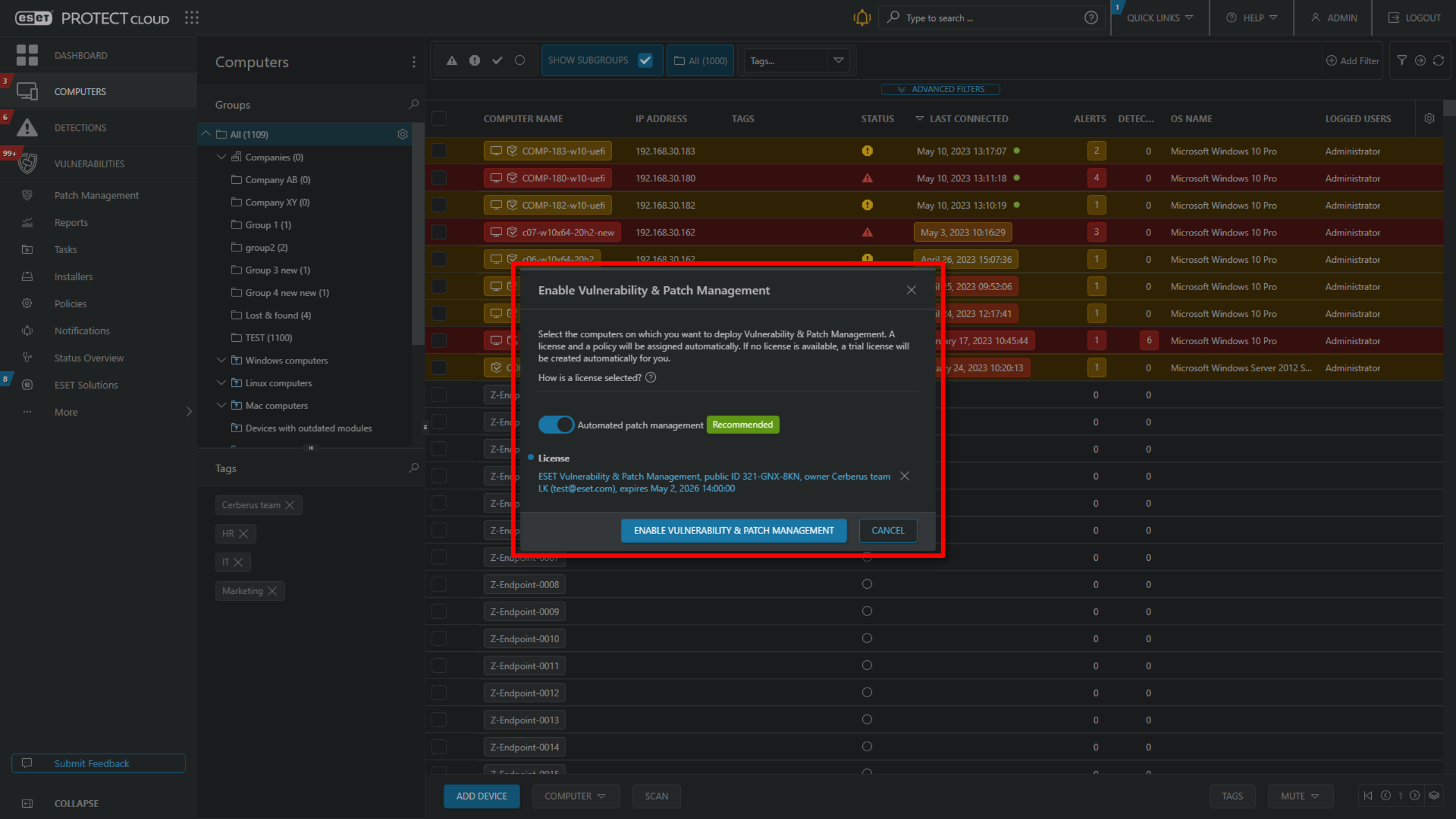
Confirmed:

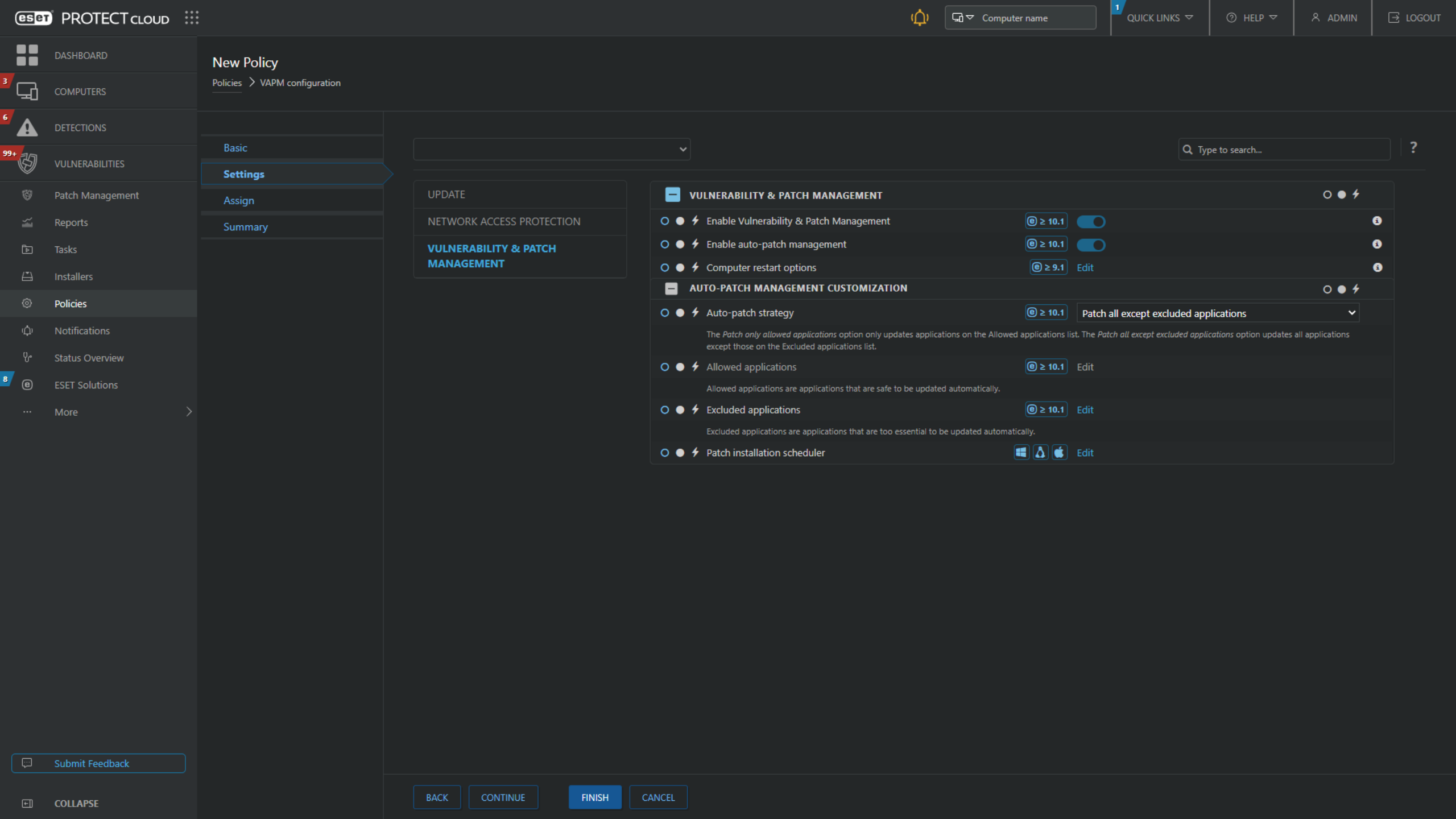
Júl 2023

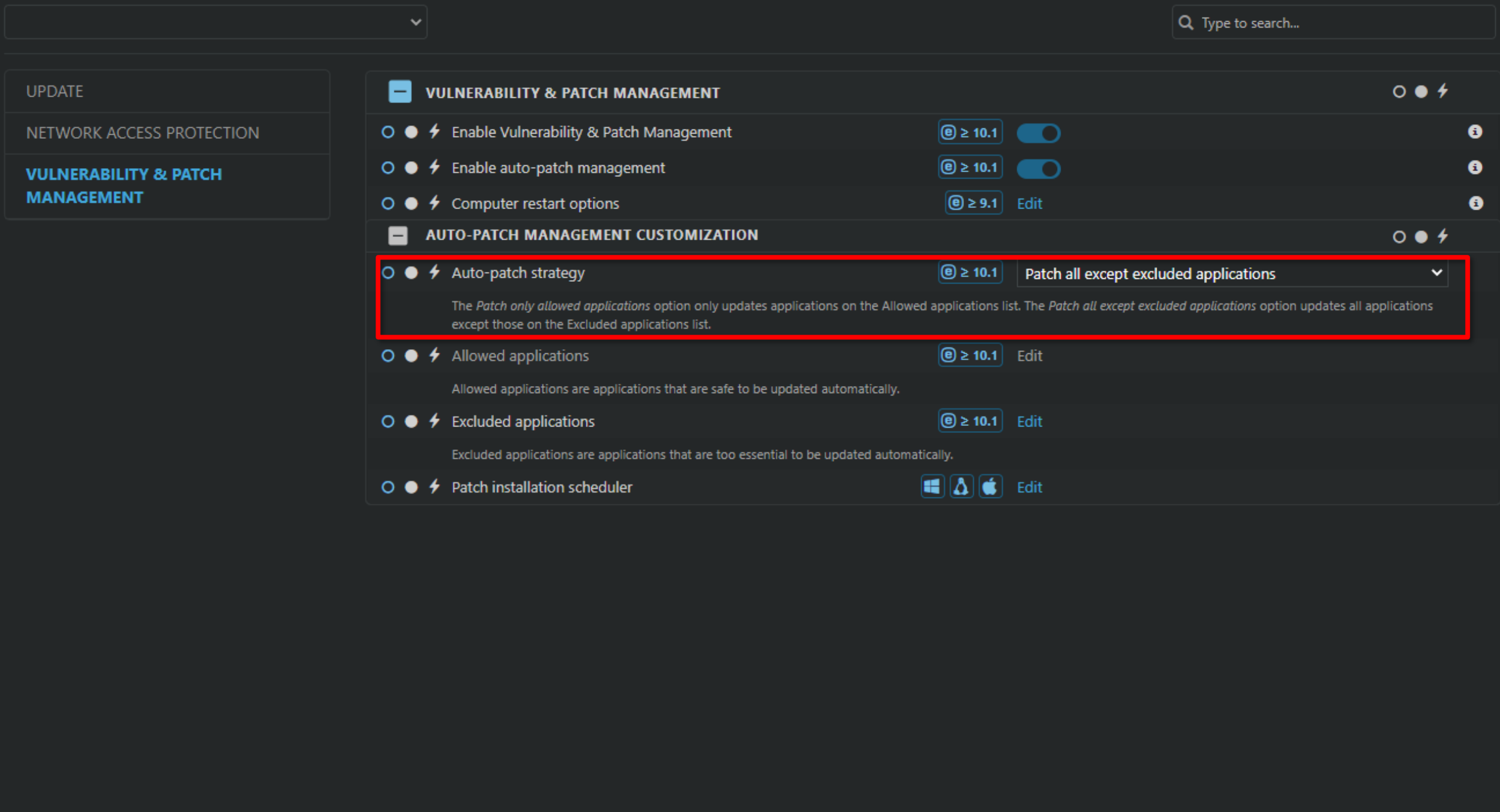
Planned:

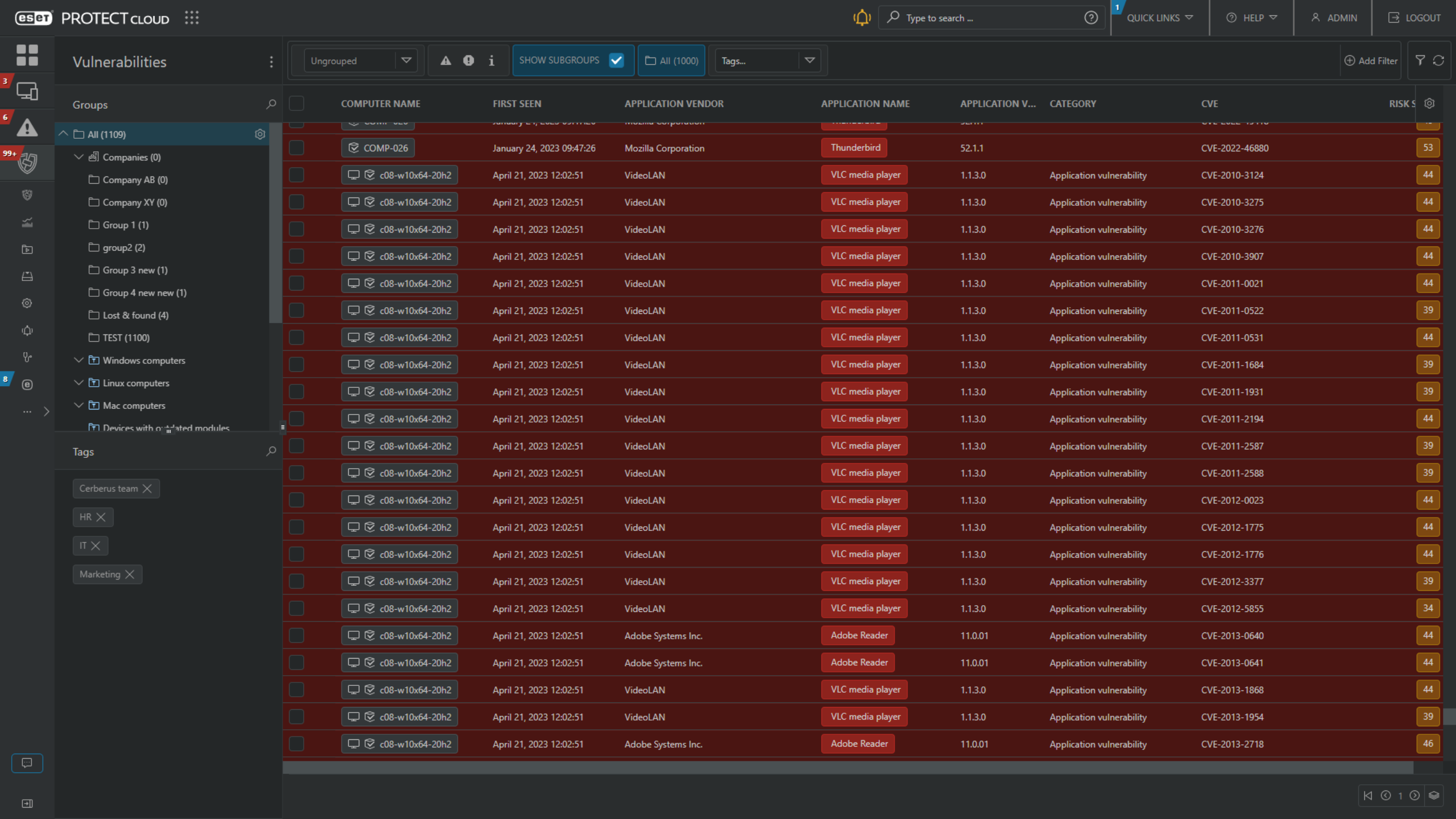
December 2023
alebo neskôr

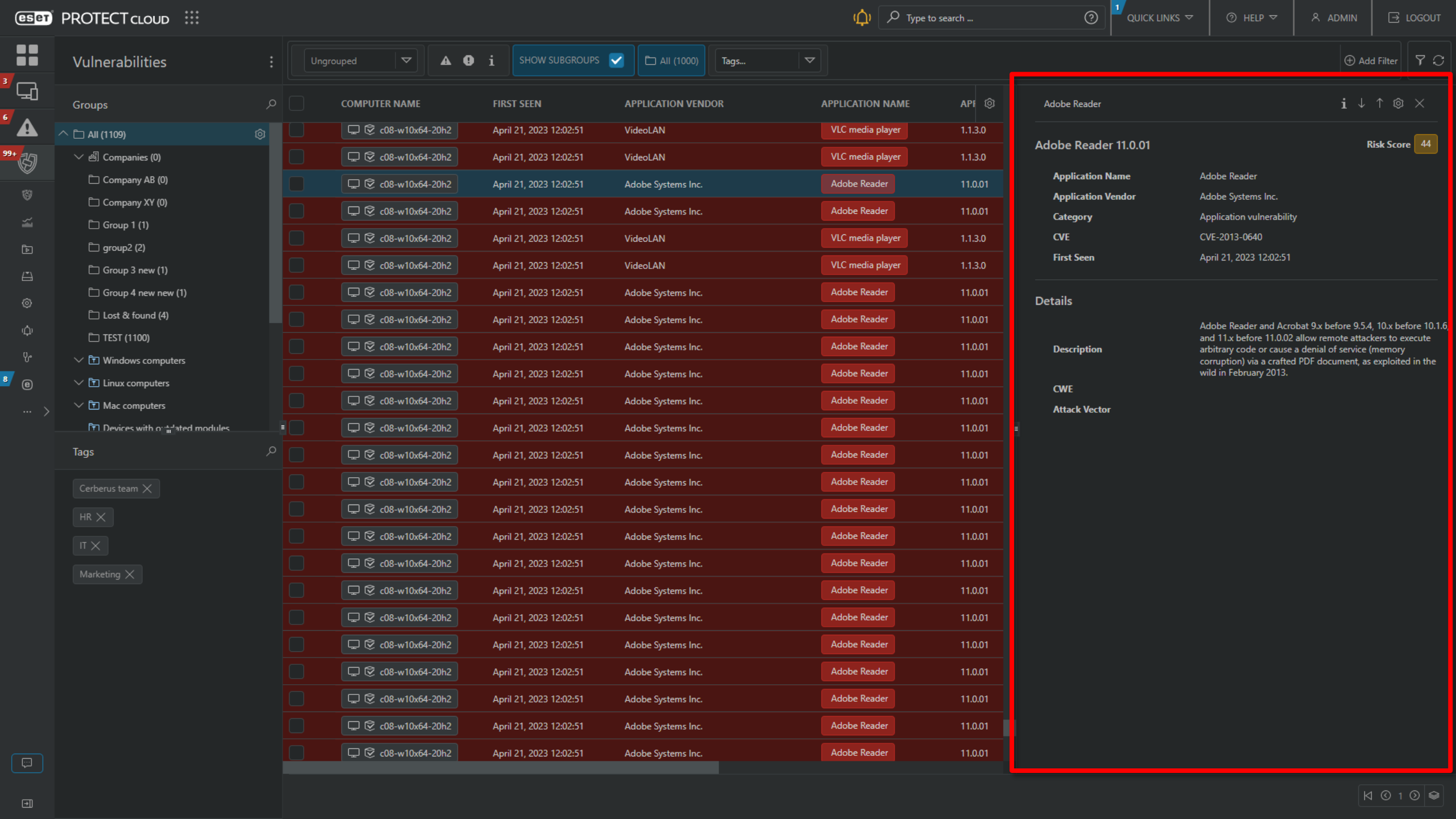

ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Computers
Groups
All (1109)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
TEST (1100)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Tags
Cerberus team
HR
IT
Marketing
SHOW SUBGROUPS
Add Filter
ADVANCED FILTERS
COMPUTER NAME
STATUS
LAST CONNECTED
ALERTS
DETEC...
OS NAME
LOGGED USERS
COMP-183-w10-uefi
May 10, 2023 13:17:07
2
0
Microsoft Windows 10 Pro
Administrator
COMP-180-w10-uefi
May 10, 2023 13:11:18
4
0
Microsoft Windows 10 Pro
Administrator
COMP-182-w10-uefi
May 10, 2023 13:10:19
1
0
Microsoft Windows 10 Pro
Administrator
c07-w10x64-20h2-new
3
0
Microsoft Windows 10 Pro
Administrator
c06-w10x64-20h2
1
0
Microsoft Windows 10 Pro
Administrator
COMP-282-w10-uefi
1
0
Microsoft Windows 10 Pro
Administrator
c08-w10x64-20h2
1
0
Microsoft Windows 10 Pro
Administrator
COMP-185win10
1
6
Microsoft Windows 10 Pro
Administrator
COMP-026
192.168.30.26
HR
January 24, 2023 10:20:13
1
0
Microsoft Windows Server 2012 S...
Administrator
Z-Endpoint-0001
Z-Endpoint-0002
Z-Endpoint-0003
Z-Endpoint-0004
Z-Endpoint-0005
Z-Endpoint-0006
Z-Endpoint-0007
Z-Endpoint-0008
Z-Endpoint-0009
Z-Endpoint-0010
Z-Endpoint-0011
Z-Endpoint-0012
Z-Endpoint-0013
Z-Endpoint-0014
Computer
Details
Investigate (Inspect)
Scan
Network Isolation
Connect via RDP
Power
Update
Solutions
Tasks
Send Wake-Up Call
Manage
Tags...
Mute
Audit Log
Solutions
Deploy security product
Deploy ESET LiveGuard
Enable Vulnerability & Patch Man...
Enable encryption
Deactivate Products
ADD DEVICE
COMPUTER
SCAN
TAGS
MUTE

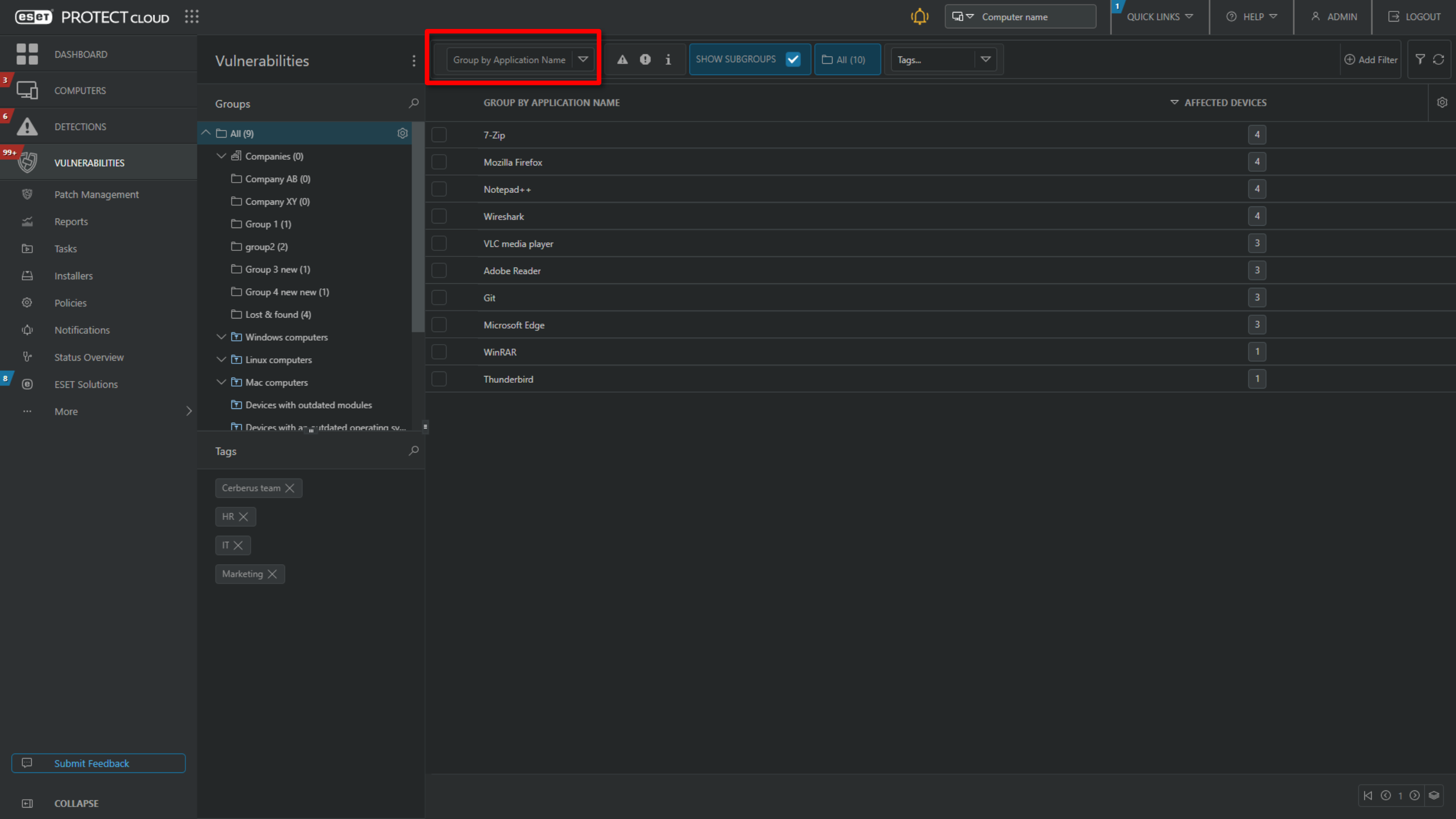

ESET PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Computers
Groups
All (1109)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
TEST (1100)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Tags
Cerberus team
HR
IT
Marketing
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
ADVANCED FILTERS
COMPUTER NAME
IP ADDRESS
TAGS
STATUS
LAST CONNECTED
ALERTS
DETEC...
OS NAME
LOGGED USERS
COMP-183-w10-uefi
192.168.30.183
May 10, 2023 13:17:07
Microsoft Windows 10 Pro
Administrator
COMP-180-w10-uefi
192.168.30.180
May 10, 2023 13:11:18
COMP-182-w10-uefi
192.168.30.182
May 10, 2023 13:10:19
c07-w10x64-20h2-new
192.168.30.162
May 3, 2023 10:16:29
Microsoft Windows Server 2012 S...
Enable Vulnerability & Patch Management
Select the computers on which you want to deploy Vulnerability & Patch Management. A license and a policy will be assigned automatically. If no license is available, a trial license will be created automatically for you.
How is a license selected?
Automated patch management
Recommended
License
ESET Vulnerability & Patch Management, public ID 321-GNX-8KN, owner Cerberus team LK (test@eset.com), expires May 2, 2026 14:00:00
ENABLE VULNERABILITY & PATCH MANAGEMENT
CANCEL
Z-Endpoint-0008
Z-Endpoint-0009
Z-Endpoint-0010
Z-Endpoint-0011
Z-Endpoint-0012
Z-Endpoint-0013
Z-Endpoint-0014
ADD DEVICE
COMPUTER
SCAN
TAGS
MUTE

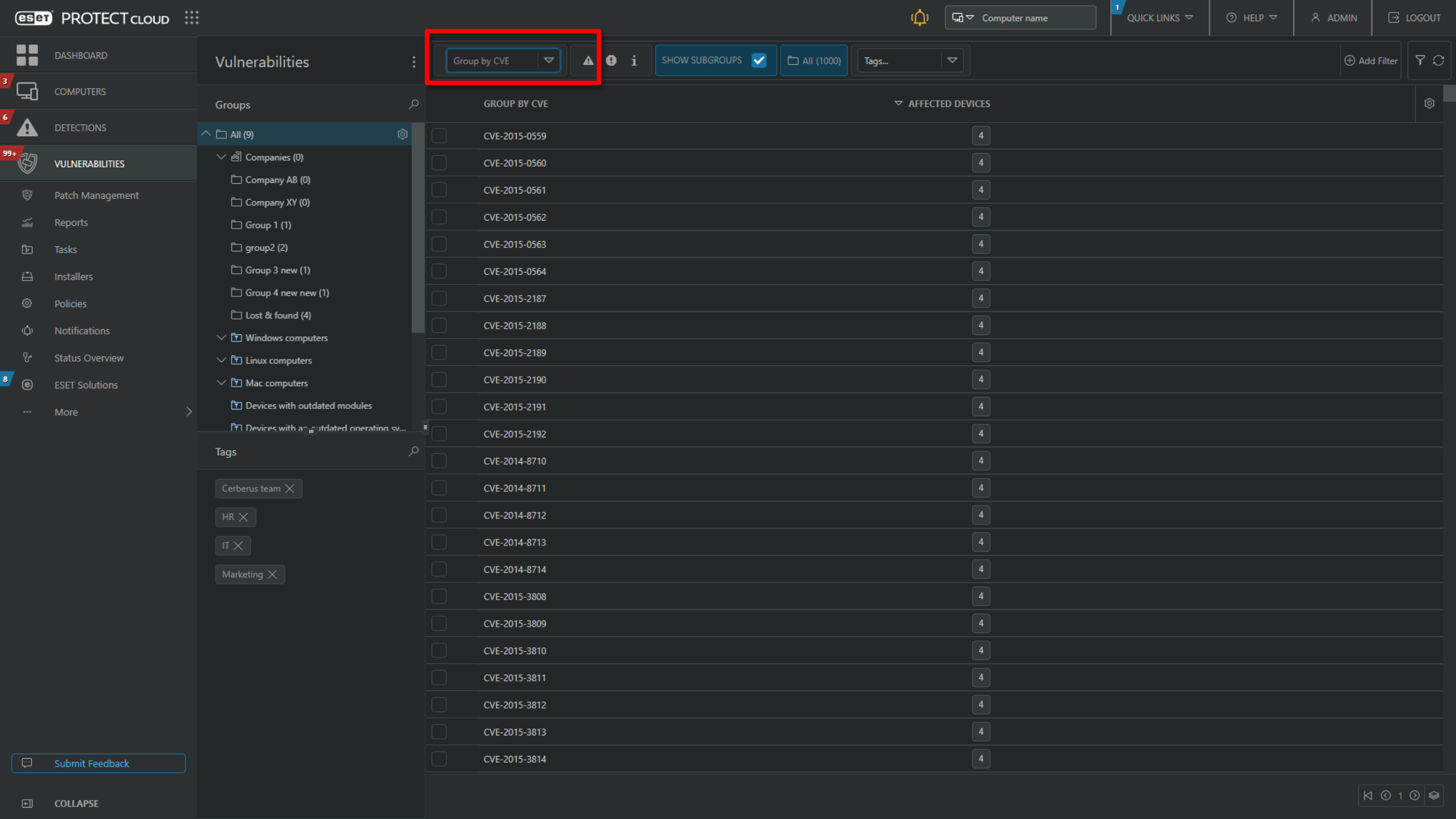

PROTECT CLOUD
Computer name
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
New Policy
Policies > VAPM configuration
Basic
Settings
Assign
Summary
Type to search...
UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT
VULNERABILITY & PATCH MANAGEMENT
Enable Vulnerability & Patch Management
≥ 10.1
Enable auto-patch management
≥ 10.1
Computer restart options
≥ 9.1
Edit
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
≥ 10.1
Patch all except excluded applications
The Patch only allowed applications option only updates applications on the Allowed applications list. The Patch all except excluded applications option updates all applications except those on the Excluded applications list.
Allowed applications
≥ 10.1
Edit
Allowed applications are applications that are safe to be updated automatically.
Excluded applications
≥ 10.1
Edit
Excluded applications are applications that are too essential to be updated automatically.
Patch installation scheduler
Edit
BACK
CONTINUE
FINISH
CANCEL

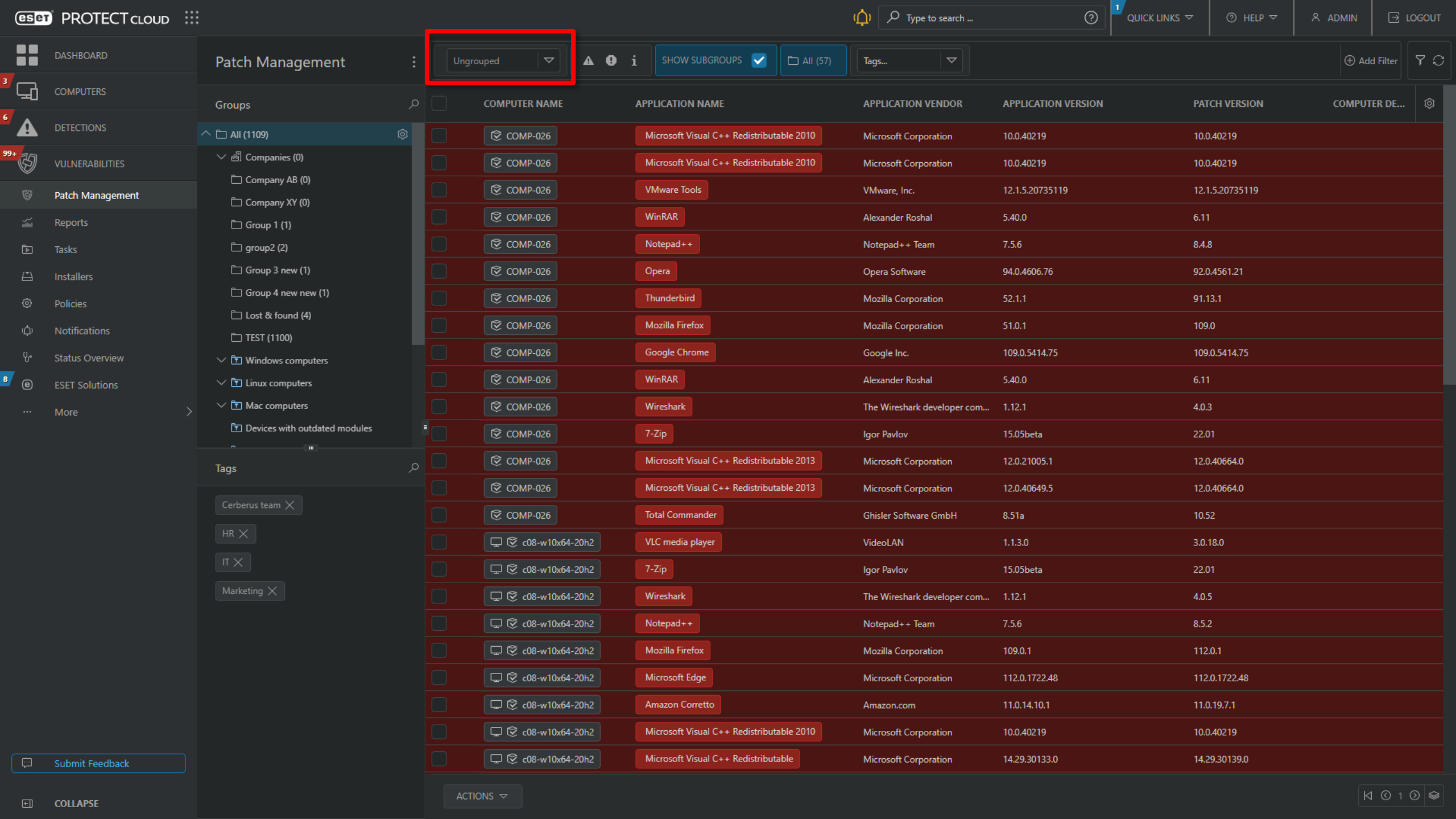

Type to search...
UPDATE
NETWORK ACCESS PROTECTION
VULNERABILITY & PATCH MANAGEMENT
VULNERABILITY & PATCH MANAGEMENT
Enable Vulnerability & Patch Management
≥ 10.1
Enable auto-patch management
≥ 10.1
Computer restart options
≥ 9.1
Edit
AUTO-PATCH MANAGEMENT CUSTOMIZATION
Auto-patch strategy
≥ 10.1
Patch all except excluded applications
The Patch only allowed applications option only updates applications on the Allowed applications list. The Patch all except excluded applications option updates all applications except those on the Excluded applications list.
Allowed applications
≥ 10.1
Edit
Allowed applications are applications that are safe to be updated automatically.
Excluded applications
≥ 10.1
Edit
Excluded applications are applications that are too essential to be updated automatically.
Patch installation scheduler
Edit

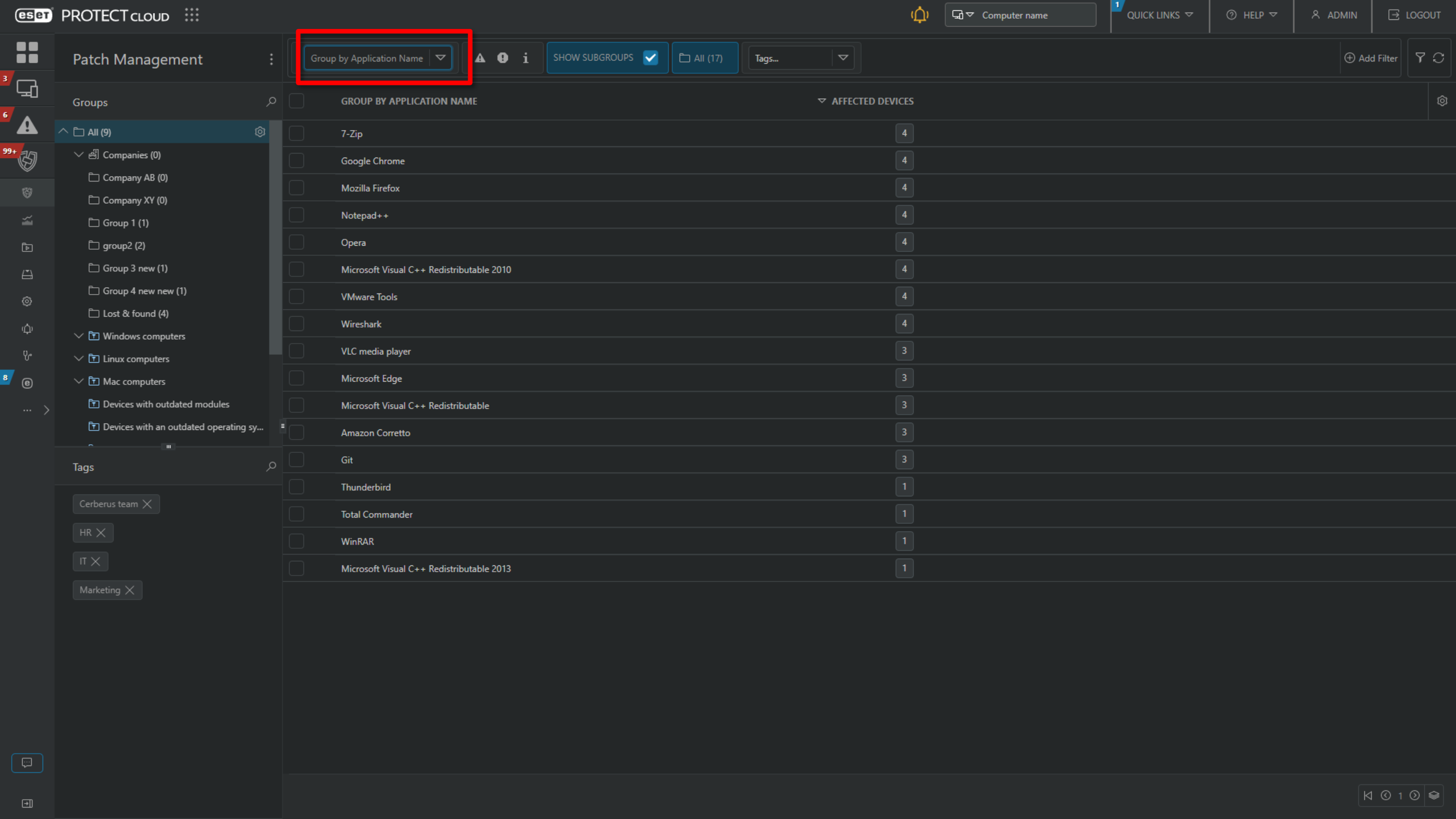

PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
ADMIN
LOGOUT
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (1109)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
TEST (1100)
Windows computers
Linux computers
Mac computers
Tags
Cerberus team
HR
IT
Marketing
COMPUTER NAME
FIRST SEEN
APPLICATION VENDOR
APPLICATION NAME
APPLICATION V...
CATEGORY
CVE
RISK S
COMP-026 January 24, 2023 09:47:26 Mozilla Corporation Thunderbird 52.1.1 CVE-2022-46880 53
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2010-3124 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2010-3275 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2010-3276 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2010-3907 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-0021 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-0522 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-0531 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-1684 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-1931 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-2194 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-2587 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2011-2588 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2012-0023 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2012-1775 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2012-1776 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2012-3377 39
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2012-5855 34
c08-w10x64-20h2 April 21, 2023 12:02:51 Adobe Systems Inc. Adobe Reader 11.0.01 Application vulnerability CVE-2013-0640 44
c08-w10x64-20h2 April 21, 2023 12:02:51 Adobe Systems Inc. Adobe Reader 11.0.01 Application vulnerability CVE-2013-0641 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2013-1868 44
c08-w10x64-20h2 April 21, 2023 12:02:51 VideoLAN VLC media player 1.1.3.0 Application vulnerability CVE-2013-1954 39
c08-w10x64-20h2 April 21, 2023 12:02:51 Adobe Systems Inc. Adobe Reader 11.0.01 Application vulnerability CVE-2013-2718 46


PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
ADMIN
LOGOUT
Vulnerabilities
Ungrouped
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (1109)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
TEST (1100)
Windows computers
Linux computers
Mac computers
Tags
Cerberus team
HR
IT
Marketing
COMPUTER NAME
FIRST SEEN
APPLICATION VENDOR
APPLICATION NAME
c08-w10x64-20h2
April 21, 2023 12:02:51
VideoLAN
VLC media player
1.1.3.0
Adobe Systems Inc.
Adobe Reader
11.0.01
Adobe Reader
Adobe Reader 11.0.01
Risk Score 44
Application Name Adobe Reader
Application Vendor Adobe Systems Inc.
Category Application vulnerability
CVE CVE-2013-0640
First Seen April 21, 2023 12:02:51
Details
Description Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6 and 11.x before 11.0.02 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, as exploited in the wild in February 2013.
CWE
Attack Vector


ESET PROTECT CLOUD
Computer name
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Vulnerabilities
Group by Application Name
SHOW SUBGROUPS
All (10)
Tags...
Add Filter
Groups
All (9)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Tags
Cerberus team
HR
IT
Marketing
GROUP BY APPLICATION NAME
AFFECTED DEVICES
7-Zip 4
Mozilla Firefox 4
Notepad++ 4
Wireshark 4
VLC media player 3
Adobe Reader 3
Git 3
Microsoft Edge 3
WinRAR 1
Thunderbird 1


PROTECT CLOUD
Computer name
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Vulnerabilities
Group by CVE
SHOW SUBGROUPS
All (1000)
Tags...
Add Filter
Groups
All (9)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Tags
Cerberus team
HR
IT
Marketing
GROUP BY CVE
AFFECTED DEVICES
CVE-2015-0559 4
CVE-2015-0560 4
CVE-2015-0561 4
CVE-2015-0562 4
CVE-2015-0563 4
CVE-2015-0564 4
CVE-2015-2187 4
CVE-2015-2188 4
CVE-2015-2189 4
CVE-2015-2190 4
CVE-2015-2191 4
CVE-2015-2192 4
CVE-2014-8710 4
CVE-2014-8711 4
CVE-2014-8712 4
CVE-2014-8713 4
CVE-2014-8714 4
CVE-2015-3808 4
CVE-2015-3809 4
CVE-2015-3810 4
CVE-2015-3811 4
CVE-2015-3812 4
CVE-2015-3813 4
CVE-2015-3814 4


PROTECT CLOUD
Type to search ...
QUICK LINKS
HELP
ADMIN
LOGOUT
DASHBOARD
COMPUTERS
DETECTIONS
VULNERABILITIES
Patch Management
Reports
Tasks
Installers
Policies
Notifications
Status Overview
ESET Solutions
More
Submit Feedback
COLLAPSE
Patch Management
Ungrouped
SHOW SUBGROUPS
All (57)
Tags...
Add Filter
Groups
All (1109)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
TEST (1100)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Tags
Cerberus team
HR
IT
Marketing
COMPUTER NAME
APPLICATION NAME
APPLICATION VENDOR
APPLICATION VERSION
PATCH VERSION
COMPUTER DE...
COMP-026 Microsoft Visual C++ Redistributable 2010 Microsoft Corporation 10.0.40219 10.0.40219
COMP-026 Microsoft Visual C++ Redistributable 2010 Microsoft Corporation 10.0.40219 10.0.40219
COMP-026 VMware Tools VMware, Inc. 12.1.5.20735119 12.1.5.20735119
COMP-026 WinRAR Alexander Roshal 5.40.0 6.11
COMP-026 Notepad++ Notepad++ Team 7.5.6 8.4.8
COMP-026 Opera Opera Software 94.0.4606.76 92.0.4561.21
COMP-026 Thunderbird Mozilla Corporation 52.1.1 91.13.1
COMP-026 Mozilla Firefox Mozilla Corporation 51.0.1 109.0
COMP-026 Google Chrome Google Inc. 109.0.5414.75 109.0.5414.75
COMP-026 WinRAR Alexander Roshal 5.40.0 6.11
COMP-026 Wireshark The Wireshark developer com... 1.12.1 4.0.3
COMP-026 7-Zip Igor Pavlov 15.05beta 22.01
COMP-026 Microsoft Visual C++ Redistributable 2013 Microsoft Corporation 12.0.21005.1 12.0.40664.0
COMP-026 Microsoft Visual C++ Redistributable 2013 Microsoft Corporation 12.0.40649.5 12.0.40664.0
COMP-026 Total Commander Ghisler Software GmbH 8.51a 10.52
c08-w10x64-20h2 VLC media player VideoLAN 1.1.3.0 3.0.18.0
c08-w10x64-20h2 7-Zip Igor Pavlov 15.05beta 22.01
c08-w10x64-20h2 Wireshark The Wireshark developer com... 1.12.1 4.0.5
c08-w10x64-20h2 Notepad++ Notepad++ Team 7.5.6 8.5.2
c08-w10x64-20h2 Mozilla Firefox Mozilla Corporation 109.0.1 112.0.1
c08-w10x64-20h2 Microsoft Edge Microsoft Corporation 112.0.1722.48 112.0.1722.48
c08-w10x64-20h2 Amazon Corretto Amazon.com 11.0.14.10.1 11.0.19.7.1
c08-w10x64-20h2 Microsoft Visual C++ Redistributable 2010 Microsoft Corporation 10.0.40219 10.0.40219
c08-w10x64-20h2 Microsoft Visual C++ Redistributable Microsoft Corporation 14.29.30133.0 14.29.30139.0
ACTIONS


PROTECT CLOUD
Computer name
QUICK LINKS
HELP
ADMIN
LOGOUT
Patch Management
Group by Application Name
SHOW SUBGROUPS
All (17)
Tags...
Add Filter
Groups
All (9)
Companies (0)
Company AB (0)
Company XY (0)
Group 1 (1)
group2 (2)
Group 3 new (1)
Group 4 new new (1)
Lost & found (4)
Windows computers
Linux computers
Mac computers
Devices with outdated modules
Devices with an outdated operating sy...
Tags
Cerberus team
HR
IT
Marketing
GROUP BY APPLICATION NAME
AFFECTED DEVICES
7-Zip 4
Google Chrome 4
Mozilla Firefox 4
Notepad++ 4
Opera 4
Microsoft Visual C++ Redistributable 2010 4
VMware Tools 4
Wireshark 4
VLC media player 3
Microsoft Edge 3
Microsoft Visual C++ Redistributable 3
Amazon Corretto 3
Git 3
Thunderbird 1
Total Commander 1
WinRAR 1
Microsoft Visual C++ Redistributable 2013 1

SECURITY DAYS

Priestor na otázky

Digital Security
Progress. Protected. & SME KONFERENCIE