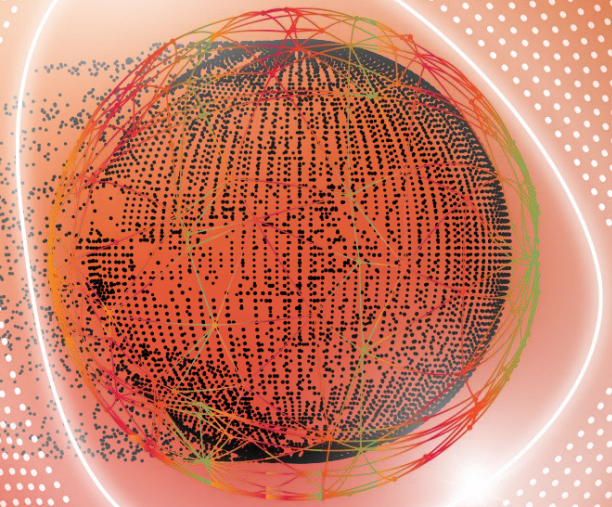


Roglit 25

Varni ali ranljivi? To je sedaj vprašanje

Partner: Exclusive Networks
Predavatelj: Tone Gorup

Zavezništvo za močnejši IT ekosistem – Building a Stronger IT Ecosystem

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Kaj so ranljivosti računalniške opreme

Ranljivosti so napake ali pomanjkljivosti v računalniški opremi, ki jih napadalec lahko izkoristi za uspešen prevzem nadzora nad računalnikom ali njegovimi komponentami

ranljivosti najdemo v

- **operacijskih sistemih**
- **aplikacijah**
- **omrežnih napravah**
- **napakah uporabnikov**

Tenable.SC in Nessus scanner
Pravi orodji za nadzor nad ranljivostmi

Roglit 25

Nessus scanner:

- **orodje za skeniranje omrežij**
- **izdelavo poročil o najdenih ranljivostih**
- **priporočila za odpravo ranljivosti**
- **ocena kritičnosti za najdene ranljivosti**
- **predloge za specifično skeniranje**
- **cca 230000 pluginov**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Tenable.SC in Nessus scanner
Pravi orodji za nadzor nad ranljivostmi

Nessus scanner lahko postavimo na:

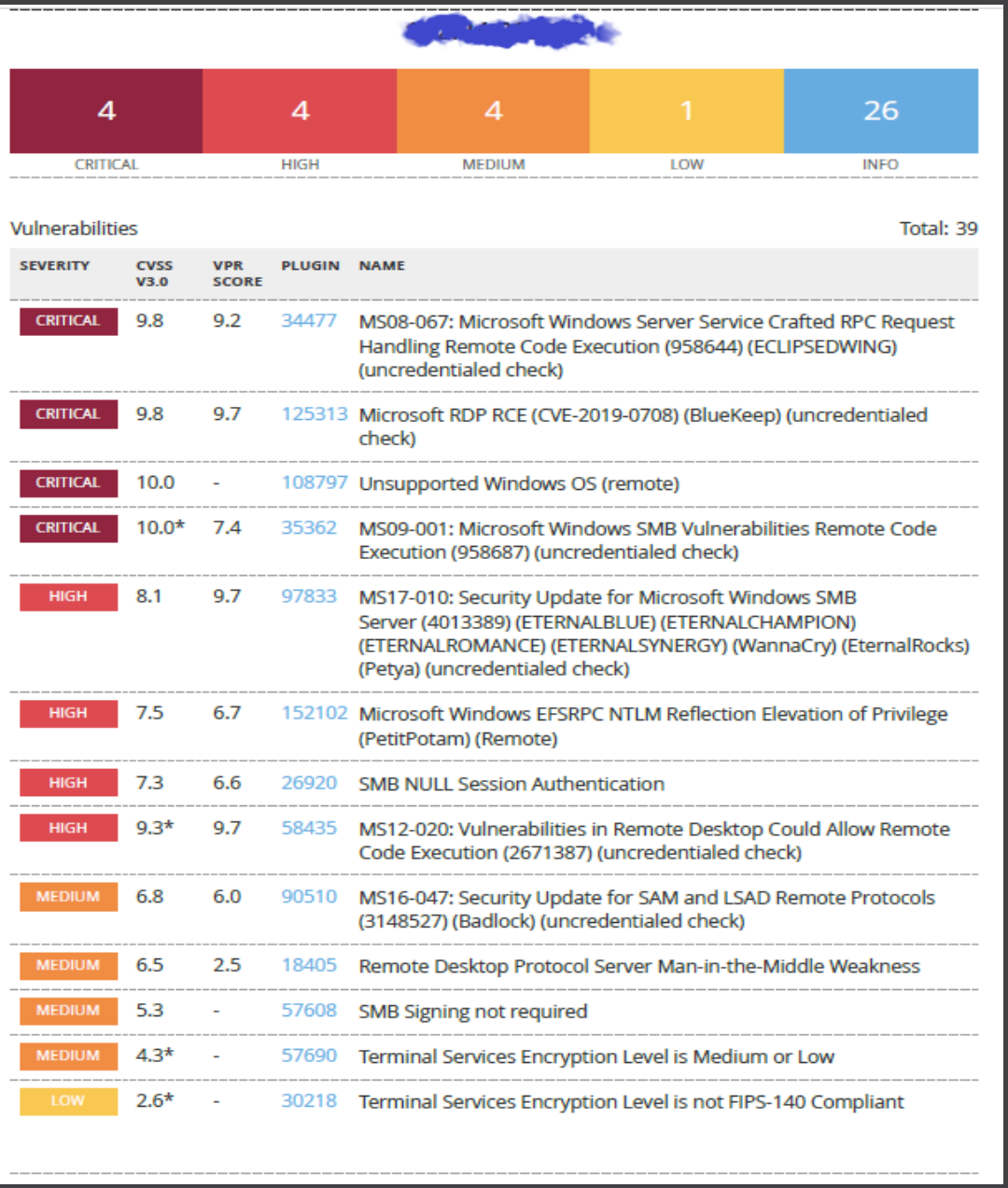
- **Windows**
- **Linux**
- **virtualni strežnik**

Uporabljamo ga za skeniranje:

- **majhnih omrežij**
- **odprtih omrežij**
- **omrežij z enostavnim dostopom**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Poročilo Nessus



4	4	4	1	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 39

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	9.8	9.7	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	6.7	152102	Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)
HIGH	7.3	6.6	26920	SMB NULL Session Authentication
HIGH	9.3*	9.7	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
MEDIUM	6.8	6.0	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	2.5	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.3*	-	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6*	-	30218	Terminal Services Encryption Level is not FIPS-140 Compliant

Tenable.SC in Nessus scanner
Pravi orodji za nadzor nad ranljivostmi

Tenable.SC:

- avtomatizirano skeniranje omrežij preko vseh skenerjev
- hramba rezultatov v interni bazi podatkov
- zelo veliko število pripravljenih poročil
- veliko različnih dashboardov za nadzor nad ranljivostmi
- spremljanje trendov

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Tenable.SC in Nessus scanner
Pravi orodji za nadzor nad ranljivostmi

Tenable.SC uporabljamo za:

- **skeniranje velikih,razvejanih omrežij**
- **stalno, periodično skeniranje**
- **analizo in primerjavo rezultatov različnih skeniranj**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Poročilo Tenable.SC

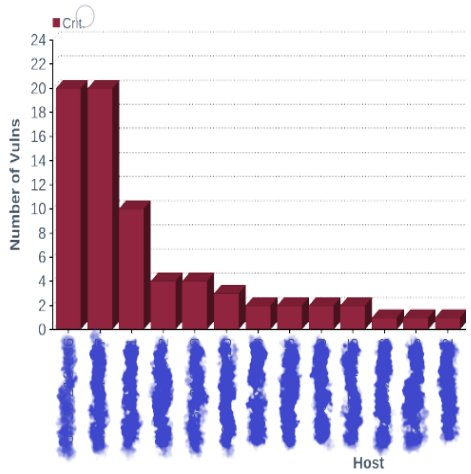
Povzetek ranljivosti z možnostjo izkoriščanja

Poglavje prikazuje povzetek najbolj kritičnih ranljivosti. Poglavje vsebuje stolpčni grafikon 20 najbolj ranljivih sistemov, tabelo 10 najbolj ranljivih sistemov s podrobnostmi o sistemu, seznam vrat in seznam najbolj kritičnih ranljivosti.

Grafikon prikazuje 20 sistemov z največ kritičnimi ranljivostmi. Vrstica predstavlja število ranljivosti, ki jih je mogoče izkoristiti, odkritih v sistemu. Ti sistemi vsebujejo znane ranljivosti, ki jih je mogoče izkoristiti, in jih je treba čim prej nadgraditi.

Tabela prikazuje matriko ranljivosti, ki jih je mogoče izkoristiti. Obstajajo 4 stolpci, ki prikazujejo skupno število ranljivosti, ki jih je mogoče izkoristiti, sledijo pa jim stolpci za stopnje kritičnosti. Vrstice so organizirane po možnostih izkoriščanja ranljivosti, vključno z novo oznako »Izkoriščanje zlonamerne programske opreme«. Prva vrstica prikazuje število ranljivosti, ki jih je mogoče izkoristiti. Naslednje vrstice so razčlenjene po možnostih izkoriščanja ranljivosti. Celice prikazujejo število ranljivosti, ki jih je mogoče izkoristiti, za vsako možnost izkoriščanja glede na kritičnost. Če ranljivosti ni, je celica označena s številko 0, ozadje je zeleno, barva pisave pa bela. Če je možno izkoristiti od 1 do 10 ranljivosti, je ozadje celice rumeno, barva pisave pa bela. Če je možno izkoristiti od 11 do 50 ranljivosti, je ozadje
v rdeči barvi. Barva pisave

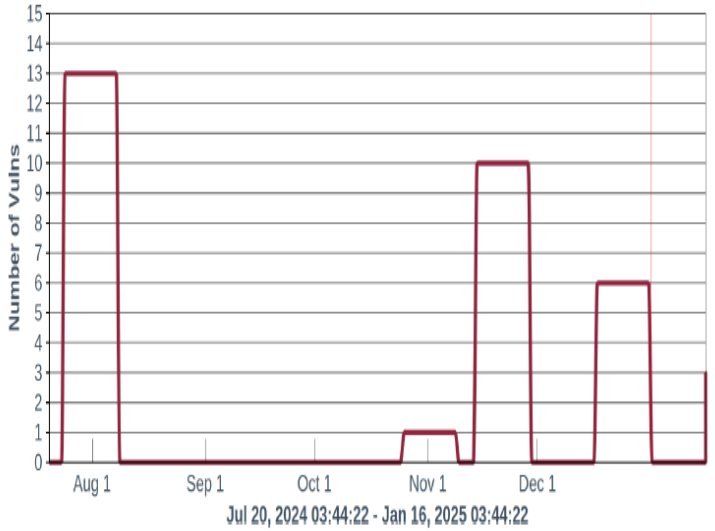
20 najbolj kritičnih sistemov



Grafi prikazujejo zgodovinski pogled na ranljivosti, odkrite na mesečni ravni. Grafi analizirajo podatke v zadnjih 6 mesecih, zajemajo rezultate vsakih 15 dni, in prikazujejo nove ranljivosti za preteklih 15 dni. Iz tega lahko vodstvo vidi trend odkrivanja ranljivosti. Ta metoda bo prikazala vrhove ranljivosti, ko pride do novih dogodkov in ko bodo v SecurityCenter končani novi pregledi. Prvi graf je za kritične ranljivosti, ki jih je mogoče izkoristiti, medtem ko drugi graf prikazuje skupno število kritičnih ranljivosti.

visoko kritične	najbolj kritične
73	81
3	0
3	5
2	0
2	0

6 - mesečni trend po mesecih (z možnostjo izkoriščanja)



Roglit 25

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Dradis – dodatno orodje za hitro izdelavo specifičnih poročil

Roglit 25

Dradis:

- **pokriva vrzel med relativno omejenim poročanjem direktno iz Nessus scannerja in obilico namenskih predpripravljenih poročil, ki jih ponuja Tenable.SC**
- **možnost hitre izdelave specifičnih poročil v Wordu**
- **integracija z Nessus scannerjem**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Poročilo Dradis

3.1.137 Apache 2.2.x < 2.2.14 Multiple Vulnerabilities

Opis:

According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.14. It is, therefore, potentially affected by multiple vulnerabilities:

- Faulty error handling in the Solaris pollset support could lead to a denial of service. (CVE-2009-2699)
- The 'mod_proxy_ftp' module allows remote attackers to bypass intended access restrictions. (CVE-2009-3095)
- The 'ap_proxy_ftp_handler' function in 'modules/proxy/proxy_ftp.c' in the 'mod_proxy_ftp' module allows remote FTP servers to cause a denial of service. (CVE-2009-3094)

Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves.

Seznam naprav na katerih je bila zaznana ranljivost:

Predlog rešitve:

Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use.

Povzetek

- ranljivosti so, so bile in bodo
- za njihovo detekcijo potrebujemo primerna orodja
- brez kvalitetnih porčil nismo naredili nič
- poročila morajobiti prilagojena naročniku
- ranljivosti je potrebno odpraviti, do takrat

pa se jih je potrebno **zavedati!!!**

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Vprašanja?

Roglit 25

Ali se spomnimo Ahila?

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company

Roglit 25

Zaključek

RoglIT is more than just another conference.

ACTUAL I.T. UNISTAR PRO ITELIS astec ACTUAL I.T. GROUP A DBA Group Company