

## Scan de Vulnérabilité

IP Address : Port		192.168.253.134:101
CVE Code(s)		CVE-2024-30850
Title		Exploit for CVE-2024-30850
Family		exploit
CVSS		0.0
Link		

-----

IP Address : Port		192.168.253.134:101
CVE Code(s)		CVE-2023-30253
Title		Exploit for OS Command Injection in Dolibarr Dolibarr
Erp/Crm		
Family		exploit
CVSS		8.8
Link		

-----

IP Address : Port		192.168.253.134:101
CVE Code(s)		CVE-2023-30253
Title		Exploit for OS Command Injection in Dolibarr Dolibarr
Erp/Crm		
Family		exploit
CVSS		8.8
Link		

-----

IP Address : Port | 192.168.253.134:101  
CVE Code(s) | CVE-2023-35813  
Title | Exploit for CVE-2023-35813  
Family | exploit  
CVSS | 9.8  
Link |

-----

IP Address : Port | 192.168.253.134:101

CVE Code(s) |  
Title | ZoomEye Search  
Family | exploit  
CVSS | 0.0  
Link |  
[https://www.rapid7.com/db/modules/auxiliary/gather/zoomeye\\_search/](https://www.rapid7.com/db/modules/auxiliary/gather/zoomeye_search/)

-----

IP Address : Port | 192.168.253.134:102

CVE Code(s) |  
Title | Siemens Simatic S7 1200 - CPU Command Module  
(Metasploit)  
Family | exploit  
CVSS | 0.0  
Link | <https://www.exploit-db.com/exploits/38964>

-----

IP Address : Port | 192.168.253.134:102

CVE Code(s) |

Title		Siemens Simatic S7 1200 CPU Command Module (MSF) Exploit
Family		exploit
CVSS		0.0
Link		<a href="https://0day.today/exploit/description/24723">https://0day.today/exploit/description/24723</a>

-----

IP Address : Port | 192.168.253.134:102

CVE Code(s) |

Title		Siemens Simatic S7 1200 - CPU Command Module (Metasploit)
-------	--	---

Family		exploit
--------	--	---------

CVSS		0.0
------	--	-----

Link		
------	--	--

-----

IP Address : Port | 192.168.253.134:102

CVE Code(s) |

Title		Siemens Simatic S7-300/400 CPU START/STOP Module
-------	--	--

Family		exploit
--------	--	---------

CVSS		0.0
------	--	-----

Link		<a href="https://packetstormsecurity.com/files/114744/Siemens-Simatic-S7-300-400-CPU-START-STOP-Module.html">https://packetstormsecurity.com/files/114744/Siemens-Simatic-S7-300-400-CPU-START-STOP-Module.html</a>
------	--	---

-----

IP Address : Port | 192.168.253.134:102

CVE Code(s)		
Title		Siemens Simatic S7-1200 CPU START/STOP Module
Family		exploit
CVSS		0.0
Link		

<https://packetstormsecurity.com/files/114746/Siemens-Simatic-S7-1200-CPU-START-STOP-Module.html>

-----

IP Address : Port		192.168.253.134:109
CVE Code(s)		
Title		Axis Communications MPQTPACS 5.20.x - Server-Side Include Daemon Remote Format String
Family		exploit
CVSS		0.0
Link		

-----

IP Address : Port		192.168.253.134:109
CVE Code(s)		
Title		Axis Communications MPQT/PACS 5.20.x - Server Side Include (SSI) Daemon Remote Format String
Family		exploit
CVSS		0.0
Link		<a href="https://0day.today/exploit/description/25439">https://0day.today/exploit/description/25439</a>

-----

IP Address : Port		192.168.253.134:109
-------------------	--	---------------------

CVE Code(s) |  
Title | Axis Communications MPQT/PACS 5.20.x -  
Server-Side Include Daemon Remote Format String  
Family | exploit  
CVSS | 0.0  
Link | <https://www.exploit-db.com/exploits/40125>

---

IP Address : Port | 192.168.253.134:109

CVE Code(s) |  
Title | Axis Communications MPQT/PACS SSI Remote  
Format String / Code Execution  
Family | exploit  
CVSS | 0.0  
Link |  
<https://packetstormsecurity.com/files/137941/Axis-Communications-MPQT-PACS-SSI-Remote-Format-String-Code-Execution.html>

---

IP Address : Port | 192.168.253.134:109

CVE Code(s) |  
Title | University of Washington pop2d 4.46/4.51/4.54/4.55  
Remote File Read Vulnerability  
Family | exploit  
CVSS | 0.0  
Link | <https://www.seebug.org/vuldb/ssvid-73979>

---

IP Address : Port | 192.168.253.134:110

CVE Code(s) |

Title | POP3 Login Utility

Family | exploit

CVSS | 0.0

Link |

[https://www.rapid7.com/db/modules/auxiliary/scanner/pop3/pop3\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/pop3/pop3_login/)

-----

IP Address : Port | 192.168.253.134:110

CVE Code(s) |

Title | Seattle Lab Mail 5.5 Denial Of Service

Family | exploit

CVSS | 0.0

Link |

<https://packetstormsecurity.com/files/176832/Seattle-Lab-Mail-5.5-Denial-Of-Service.html>

-----

IP Address : Port | 192.168.253.134:110

CVE Code(s) |

Title | MailCarrier 2.51 Denial Of Service Exploit

Family | exploit

CVSS | 0.0

Link | <https://0day.today/exploit/description/39247>

-----

IP Address : Port | 192.168.253.134:110

CVE Code(s)		
Title		MailCarrier 2.51 Denial Of Service
Family		exploit
CVSS		0.0
Link		

<https://packetstormsecurity.com/files/176555/MailCarrier-2.51-Denial-Of-Service.html>

-----

IP Address : Port		192.168.253.134:110
CVE Code(s)		
Title		Authentication Capture: SMTP
Family		exploit
CVSS		0.0
Link		

<https://www.rapid7.com/db/modules/auxiliary/server/capture/smtp/>

-----

IP Address : Port		192.168.253.134:111
CVE Code(s)		
Title		MiniDVBLinux &lt;=5.4 - Config Download Exploit
Family		exploit
CVSS		0.0
Link		<a href="https://www.exploit-db.com/exploits/51091">https://www.exploit-db.com/exploits/51091</a>

-----

IP Address : Port		192.168.253.134:111
CVE Code(s)		

Title		MiniDVBLinux 5.4 Configuration Download
Family		exploit
CVSS		0.0
Link		

<https://packetstormsecurity.com/files/168731/MiniDVBLinux-5.4-Configuration-Download.html>

-----

IP Address : Port | 192.168.253.134:111

CVE Code(s) |

Title		MiniDVBLinux 5.4 Config Download Exploit
-------	--	--

Family		exploit
--------	--	---------

CVSS		0.0
------	--	-----

Link		
------	--	--

<http://zeroscience.mk/en/vulnerabilities/ZSL-2022-5713.php>

-----

IP Address : Port | 192.168.253.134:111

CVE Code(s) | CVE-2021-41773, CVE-2021-42013

Title		Exploit for Path Traversal in Apache Http Server
-------	--	--

Family		exploit
--------	--	---------

CVSS		7.5
------	--	-----

Link		
------	--	--

IP Address : Port | 192.168.253.134:111

CVE Code(s) | CVE-2021-41773

Title		Exploit for Path Traversal in Apache Http Server
-------	--	--



Family		exploit
CVSS		4.3
Link		

-----

IP Address : Port		192.168.253.134:113
-------------------	--	---------------------

CVE Code(s)		CVE-2008-5161
-------------	--	---------------

Title		SSH Version Scanner
-------	--	---------------------

Family		exploit
--------	--	---------

CVSS		2.6
------	--	-----

Link		
------	--	--

		<a href="https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_version/">https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_version/</a>
--	--	---

-----

IP Address : Port		192.168.253.134:113
-------------------	--	---------------------

CVE Code(s)		
-------------	--	--

Title		Microsoft SQL Server SUSER_SNAME Windows Domain Account Enumeration
-------	--	---

Family		exploit
--------	--	---------

CVSS		0.0
------	--	-----

Link		
------	--	--

		<a href="https://www.rapid7.com/db/modules/auxiliary/admin/mssql/mssql_enum_domain_accounts/">https://www.rapid7.com/db/modules/auxiliary/admin/mssql/mssql_enum_domain_accounts/</a>
--	--	---

-----

IP Address : Port		192.168.253.134:113
-------------------	--	---------------------

CVE Code(s)		CVE-2021-3156, CVE-2022-39046, CVE-2023-6246
-------------	--	--

Title		glibc syslog() Heap-Based Buffer Overflow Exploit
-------	--	---

Family		exploit
CVSS		8.4
Link		<a href="https://0day.today/exploit/description/39291">https://0day.today/exploit/description/39291</a>

-----

IP Address : Port		192.168.253.134:113
CVE Code(s)		CVE-2021-3156, CVE-2022-39046, CVE-2023-6246, CVE-2023-6779, CVE-2023-6780
Title		glibc syslog() Heap-Based Buffer Overflow
Family		exploit
CVSS		7.2
Link		<a href="https://packetstormsecurity.com/files/176932/glibc-syslog-Heap-Based-Buffer-Overflow.html">https://packetstormsecurity.com/files/176932/glibc-syslog-Heap-Based-Buffer-Overflow.html</a>

-----

IP Address : Port		192.168.253.134:113
CVE Code(s)		CVE-2018-2392, CVE-2018-2393
Title		SAP Internet Graphics Server (IGS) XMLCHART XXE
Family		exploit
CVSS		7.5
Link		<a href="https://www.rapid7.com/db/modules/auxiliary/admin/sap/sap_igs_xmlchart_xxe/">https://www.rapid7.com/db/modules/auxiliary/admin/sap/sap_igs_xmlchart_xxe/</a>

-----

IP Address : Port		192.168.253.134:115
CVE Code(s)		CVE-2024-4040

Title		Exploit for Code Injection in Crushftp
Family		exploit
CVSS		10.0
Link		

-----

IP Address : Port		192.168.253.134:115
CVE Code(s)		CVE-2024-4040
Title		Exploit for Code Injection in Crushftp
Family		exploit
CVSS		10.0
Link		

-----

IP Address : Port		192.168.253.134:115
CVE Code(s)		CVE-2024-4040
Title		Exploit for Code Injection in Crushftp
Family		exploit
CVSS		10.0
Link		

-----

IP Address : Port		192.168.253.134:115
CVE Code(s)		CVE-2023-38950, CVE-2023-38951, CVE-2023-38952
Title		BioTime Directory Traversal / Remote Code Execution Exploit
Family		exploit

CVSS | 9.8

Link | <https://0day.today/exploit/description/39506>

---

IP Address : Port | 192.168.253.134:115

CVE Code(s) | CVE-2023-38950, CVE-2023-38951,  
CVE-2023-38952

Title | BioTime Directory Traversal / Remote Code Execution

Family | exploit

CVSS | 7.5

Link | <https://packetstormsecurity.com/files/177859/BioTime-Directory-Traversal-Remote-Code-Execution.html>

---