telecom

BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Análisis de Vulnerabilidades - Interno

Informe Ejecutivo

04/11/2025

Tabla de Contenidos

Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Análisis de Vulnerabilidades** sobre la infraestructura de **BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **02/09/2025** y el **01/10/2025**.

Alcance

Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Análisis de Vulnerabilidades.

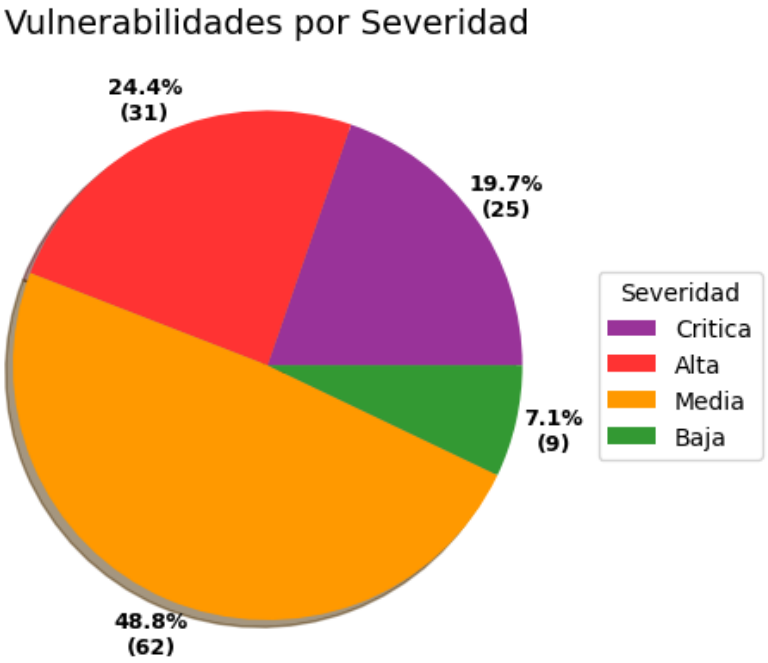
10.0.1.100
10.0.1.101
10.0.1.106
10.0.1.107
10.0.1.108
10.0.1.109
10.0.1.125
10.0.1.126
10.0.1.129
10.0.1.138
10.0.1.140
10.0.1.147
10.0.1.148
10.0.1.149
10.0.1.150
10.0.1.151
10.0.1.152
10.0.1.157
10.0.1.159
10.0.1.16
10.0.1.160
10.0.1.161
10.0.1.166
10.0.1.167
10.0.1.186
10.0.1.192
10.0.1.193
10.0.1.199
10.0.1.203
10.0.1.204
10.0.1.208
10.0.1.209
10.0.1.214
10.0.1.22
10.0.1.220
10.0.1.221
10.0.1.223
10.0.1.229
10.0.1.24
10.0.1.244
10.0.1.245
10.0.1.246
10.0.1.251
10.0.1.27
10.0.1.32
10.0.1.34
10.0.1.36
10.0.1.39
10.0.1.4
10.0.1.40
10.0.1.45
10.0.1.47
10.0.1.48
10.0.1.49
10.0.1.51
10.0.1.57
10.0.1.63
10.0.1.64
10.0.1.68
10.0.1.71
10.0.1.74
10.0.1.75
10.0.1.76
10.0.1.79
10.0.1.80
10.0.1.81
10.0.1.82
10.0.1.83
10.0.1.87
10.0.1.91
10.0.1.95
10.0.1.98
10.0.10.10
10.0.10.11
10.0.10.12
10.0.10.128
10.0.10.129
10.0.10.13
10.0.10.130
10.0.10.131

10.0.10.136
10.0.10.137
10.0.10.139
10.0.10.14
10.0.10.158
10.0.10.159
10.0.10.160
10.0.10.161
10.0.10.162
10.0.10.163
10.0.10.26
10.0.10.27
10.0.10.28
10.0.10.41
10.0.10.42
10.0.10.5
10.0.10.6
10.0.10.7
10.0.10.8
10.0.10.82
10.0.10.88
10.0.10.9
10.0.2.1
10.0.2.104
10.0.2.113
10.0.2.122
10.0.2.133
10.0.2.152
10.0.2.153
10.0.2.154
10.0.2.175
10.0.2.181
10.0.2.185
10.0.2.187
10.0.2.188
10.0.2.189
10.0.2.191
10.0.2.192
10.0.2.195
10.0.2.196
10.0.2.20
10.0.2.205
10.0.2.206
10.0.2.209
10.0.2.211
10.0.2.217
10.0.2.218
10.0.2.219
10.0.2.221
10.0.2.227
10.0.2.228
10.0.2.229
10.0.2.230
10.0.2.231
10.0.2.232
10.0.2.234
10.0.2.24
10.0.2.244
10.0.2.245
10.0.2.246
10.0.2.247
10.0.2.248
10.0.2.249
10.0.2.25
10.0.2.250
10.0.2.251
10.0.2.252
10.0.2.253
10.0.2.254
10.0.2.27
10.0.2.28
10.0.2.29
10.0.2.32
10.0.2.36
10.0.2.49
10.0.2.6
10.0.2.63
10.0.2.70
10.0.2.75
10.0.2.85
10.0.2.91
10.0.2.95
10.0.2.96
10.0.2.97
10.0.2.98
10.0.3.10
10.0.3.104
10.0.3.109
10.0.3.11
10.0.3.110
10.0.3.113
10.0.3.116
10.0.3.117
10.0.3.12
10.0.3.120
10.0.3.121
10.0.3.122
10.0.3.123
10.0.3.124
10.0.3.125
10.0.3.127
10.0.3.133
10.0.3.134
10.0.3.135
10.0.3.136
10.0.3.145
10.0.3.15
10.0.3.152
10.0.3.155
10.0.3.160
10.0.3.165
10.0.3.175

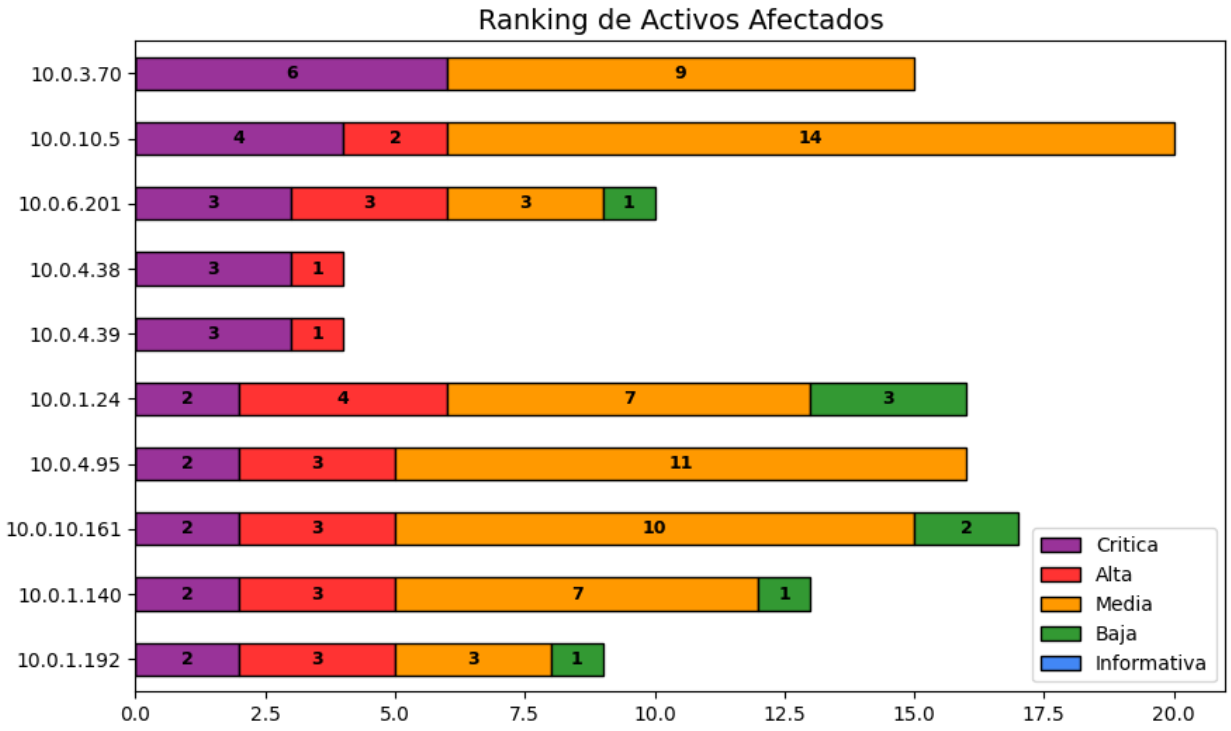
10.0.3.180
10.0.3.190
10.0.3.2
10.0.3.201
10.0.3.244
10.0.3.3
10.0.3.35
10.0.3.43
10.0.3.47
10.0.3.48
10.0.3.5
10.0.3.57
10.0.3.58
10.0.3.65
10.0.3.68
10.0.3.7
10.0.3.70
10.0.3.75
10.0.3.77
10.0.3.79
10.0.3.83
10.0.3.85
10.0.3.94
10.0.3.96
10.0.4.109
10.0.4.112
10.0.4.113
10.0.4.114
10.0.4.115
10.0.4.116
10.0.4.120
10.0.4.122
10.0.4.127
10.0.4.130
10.0.4.131
10.0.4.133
10.0.4.134
10.0.4.135
10.0.4.138
10.0.4.140
10.0.4.149
10.0.4.150
10.0.4.154
10.0.4.155
10.0.4.156
10.0.4.163
10.0.4.166
10.0.4.170
10.0.4.171
10.0.4.173
10.0.4.175
10.0.4.201
10.0.4.212
10.0.4.213
10.0.4.214
10.0.4.230
10.0.4.30
10.0.4.32
10.0.4.38
10.0.4.39
10.0.4.44
10.0.4.48
10.0.4.5
10.0.4.58
10.0.4.59
10.0.4.62
10.0.4.69
10.0.4.71
10.0.4.72
10.0.4.77
10.0.4.79
10.0.4.8
10.0.4.82
10.0.4.83
10.0.4.88
10.0.4.89
10.0.4.92
10.0.4.95
10.0.4.97
10.0.6.10
10.0.6.201
10.0.6.205
10.0.6.21
10.0.6.22
10.0.6.25
10.0.6.26
10.0.6.28
10.0.6.3
10.0.6.30
10.0.6.33
10.0.6.34
10.0.6.37
10.0.6.38
10.0.6.41
10.0.6.42
10.0.6.44
10.0.6.45
10.0.6.9
10.0.7.10
10.0.7.11
10.0.7.12
10.0.7.13
10.0.7.14

Resumen

Como resultado del análisis realizado se han identificado **127** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **25** de severidad crítica, **31** de severidad alta, **62** de severidad media y **9** de severidad baja.



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades detectadas.



Resumen de hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#1	EOL/Obsolete Software: Microsoft SQL Server 2014 Service Pack 2 (SP2) Detected	Critica	1
#2	PHP Versions Prior to 5.2.12 Multiple Vulnerabilities	Critica	4
#3	HPE Integrated Lights-Out 4 Remote Code Execution Vulnerability	Critica	3
#4	EOL/Obsolete Software: Nginx 1.x.x Detected	Critica	1
#5	Potential TCP Backdoor	Critica	53
#6	EOL/Obsolete Operating System: Microsoft Windows XP Detected	Critica	1
#7	Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) and Shadow Brokers (ECLIPSEDWING)	Critica	1
#8	Intelligent Platform Management Interface (IPMI) Detected	Critica	20
#9	Oracle Database July 2017 Patch Set Update (PSU) 12.2.0.1.170718 Not Installed (Patch 26123830)	Critica	1
#10	Oracle Database 12.2.0.1 Critical Patch Update - July 2021 (Unauthenticated)	Critica	1
#11	Oracle Database October 2017 Patch Set Update (PSU) 12.2.0.1.171017 Not Installed (Patch 26636004)	Critica	1
#12	Oracle Database 12.2.0.1 July 2020 Critical Patch Update (Unauthenticated)	Critica	1
#13	Oracle Database 12.2.0.1 Critical Patch Update - October 2020 (Unauthenticated)	Critica	1
#14	Nginx Integer Buffer Overflow Vulnerability (CVE-2017-20005)	Critica	1
#15	Rsync Multiple Vulnerabilities	Critica	3
#16	HPE Integrated Lights-Out Multiple Remote Vulnerabilities	Critica	1
#17	Apache Tomcat Multiple Vulnerabilities	Critica	1
#18	Nginx Use After Free Vulnerability (CVE-2016-0746)	Critica	1
#19	OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent	Critica	48
#20	OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908)	Critica	9
#21	Windows SMB Version 1 (SMBv1) Detected	Critica	3
#22	EOL/Obsolete Software: Oracle Database Version 12.2.0.1 Detected	Critica	4
#23	Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.60 Multiple Security Vulnerabilities	Critica	5
#24	OpenSSH Sensitive Information Disclosure Vulnerability	Critica	5
#25	Apache Tomcat Multiple Vulnerabilities	Critica	1
#26	Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021	Alta	2
#27	EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected	Alta	7
#28	EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected	Alta	2
#29	OpenSSH Multiple Vulnerabilities	Alta	1
#30	SSL Server Supports Weak Encryption Vulnerability	Alta	2

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#31	EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected	Alta	3
#32	OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion)	Alta	5
#33	EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected	Alta	1
#34	Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742)	Alta	1
#35	OpenSSH 7.4 Not Installed Multiple Vulnerabilities	Alta	1
#36	OpenSSH Integer overflow Vulnerability	Alta	4
#37	Microsoft DNS Server Recursive Query Denial of Service	Alta	7
#38	OpenSSH sshd Function Vulnerability (CVE-2015-8325)	Alta	6
#39	Windows Workstation Service NetrWkstaUserEnum Denial of Service - Zero Day	Alta	1
#40	Nginx Arbitrary Code Execution Vulnerability	Alta	1
#41	OpenSSH Security Update (CVE-2024-39894)	Alta	1
#42	Microsoft Windows UPnP NOTIFY Buffer Overflow Vulnerability (MS01-059)	Alta	1
#43	PostgreSQL Arbitrary SQL Code Execution Vulnerability (CVE-2024-7348)	Alta	1
#44	SAP ASE (Sybase ASE) "probe" Login Access Vulnerability	Alta	3
#45	PHP OpenSSL Extension Remote Memory Corruption Vulnerability	Alta	3
#46	Nginx Remote Integer Overflow Vulnerability	Alta	1
#47	IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability	Alta	3
#48	Readable SNMP Information	Alta	2
#49	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	Alta	55
#50	OpenSSH J-PAKE Session Key Retrieval Vulnerability	Alta	1
#51	OpenSSH SCP File Overwrite Vulnerability (CVE-2020-12062)	Alta	1
#52	Potential Litmus Backdoor Detected	Alta	1
#53	OpenSSH Command Injection Vulnerability	Alta	17
#54	EOL/Obsolete Software: jQuery 1.x and 2.x Detected	Alta	2
#55	Remote Management Service Accepting Unencrypted Credentials Detected (FTP)	Alta	6
#56	OpenSSH Authentication Bypass Vulnerability	Alta	23
#57	OpenSSH Multiple Security Vulnerabilities	Media	24
#58	Apache Zookeeper Common/Default Nodes Accessible Without ACL	Media	2
#59	Session Cookie Does Not Contain the "Secure" Attribute	Media	1
#60	HPE Integrated Lights-Out Remote Disclosure of Information Vulnerability	Media	1
#61	SSL Certificate - Self-Signed Certificate	Media	44
#62	SSL Certificate - Invalid Maximum Validity Date Detected	Media	137
#63	SSL Certificate - Expired	Media	6
#64	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	Media	58

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#65	Deprecated SSH Cryptographic Settings	Media	18
#66	OpenSSH Multiple Vulnerabilities	Media	31
#67	SSL Certificate - Signature Verification Failed Vulnerability	Media	152
#68	SSL Certificate - Improper Usage Vulnerability	Media	17
#69	OpenSSH server 9.1 'sshd(8)' Double-Free Vulnerability	Media	1
#70	EOL/Obsolete Software: SNMP Protocol Version Detected	Media	2
#71	OpenSSH Xauth Command Injection Vulnerability	Media	1
#72	OpenSSH Multiple CRLF injection Vulnerability (CVE-2016-3115)	Media	6
#73	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure	Media	5
#74	Encrypted Management Interfaces Accessible On Cisco Device	Media	2
#75	SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	Media	13
#76	TLS Protocol Session Renegotiation Security Vulnerability	Media	1
#77	SMBv2 Signing Not Required	Media	62
#78	Nginx Uncontrolled Resource Consumption Vulnerability (CVE-2018-16845)	Media	1
#79	Nginx Denial of Service (DoS) Vulnerability	Media	1
#80	jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability	Media	2
#81	jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability	Media	2
#82	jQuery Cross-Site Scripting (XSS) Vulnerability	Media	2
#83	OpenSSH Security Update (CVE-2025-26466)	Media	1
#84	SSH Prefix Truncation Vulnerability (Terrapin)	Media	19
#85	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)	Media	30
#86	SSL Server Has SSLv2 Enabled Vulnerability	Media	3
#87	OpenSSH Denial of Service (DoS) Vulnerability	Media	1
#88	Web Server Uses Plain-Text Form Based Authentication	Media	1
#89	Nginx HTTP Request Smuggling Vulnerability	Media	1
#90	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)	Media	2
#91	OpenSSH Improper Restriction of Operations Vulnerability	Media	1
#92	OpenSSH User Enumeration	Media	4
#93	SSH Server Public Key Too Small	Media	10
#94	OpenSSH Improper Input Validation Vulnerability	Media	2
#95	SNMP GETBULK Reflected Distributed Denial-of-Service Vulnerability	Media	2
#96	X.509 Certificate SHA1 Signature Collision Vulnerability	Media	4
#97	SSL Server Has SSLv3 Enabled Vulnerability	Media	16
#98	HTTP Security Header Not Detected	Media	9
#99	Deprecated Public Key Length	Media	8
#100	Web Server Reveals Absolute Path	Media	1
#101	TCP Test-Services	Media	1

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#102	Account Brute Force Possible Through IIS NTLM Authentication Scheme	Media	2
#103	ASP.NET DEBUG Method Enabled Security Issue	Media	1
#104	Hidden RPC Services	Media	4
#105	Microsoft Windows NT RPC Endpoint Mapper Denial of Service Vulnerability (MS01-048)	Media	51
#106	Microsoft Remote Procedure Call Service Denial of Service Vulnerability (MS01-041)	Media	51
#107	Reverse DNS Name Resolution Discloses Private Network Addresses	Media	1
#108	Global User List Found Using Other QIDS	Media	5
#109	X Display Manager Control Protocol (XDMCP) Detected	Media	2
#110	UDP Source Port Pass Firewall	Media	9
#111	Web Directories Listable Vulnerability	Media	1
#112	IP Spoofing	Media	2
#113	Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness (MS03-034)	Media	3
#114	Weak SSL/TLS Key Exchange	Media	36
#115	Apache Web Server ETag Header Information Disclosure Weakness	Media	1
#116	Web Server Uses Plain Text Basic Authentication	Media	1
#117	OpenSSH "X SECURITY" Bypass Vulnerability	Media	3
#118	NetBIOS Shared Folder List Available	Media	1
#119	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability	Baja	1
#120	OpenSSH Public-Key Authentication Vulnerability	Baja	31
#121	SHA1 deprecated setting for SSH	Baja	39
#122	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)	Baja	63
#123	OpenSSH Commands Information Disclosure Vulnerability	Baja	1
#124	Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake)	Baja	2
#125	AutoComplete Attribute Not Disabled for Password in Form Based Authentication	Baja	1
#126	NTP Information Disclosure Vulnerability	Baja	2
#127	OpenSSH Information Disclosure Vulnerability	Baja	1

Conclusiones y recomendaciones finales

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
Aplicar parches o actualizar el software obsoleto o con vulnerabilidades conocidas a las versiones recomendadas por los fabricantes.	Critica	#1 EOL/Obsolete Software: Microsoft SQL Server 2014 Service Pack 2 (SP2) Detected
	Critica	#5 PHP Versions Prior to 5.2.12 Multiple Vulnerabilities
	Critica	#21 Nginx Integer Buffer Overflow Vulnerability (CVE-2017-20005)
	Critica	#38 OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent
	Critica	#39 OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908)
	Critica	#42 Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.60 Multiple Security Vulnerabilities
	Critica	#43 OpenSSH Sensitive Information Disclosure Vulnerability
	Alta	#51 Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021
	Alta	#54 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected
	Alta	#55 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected
	Alta	#57 OpenSSH Multiple Vulnerabilities
	Alta	#65 EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected
	Alta	#67 OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion)
	Alta	#68 EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected
	Alta	#70 Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742)
	Alta	#125 OpenSSH Command Injection Vulnerability
	Alta	#129 EOL/Obsolete Software: jQuery 1.x and 2.x Detected
	Alta	#134 OpenSSH Authentication Bypass Vulnerability
	Media	#158 OpenSSH Multiple Vulnerabilities

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
	Media	#180 jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability
	Media	#187 SSH Prefix Truncation Vulnerability (Terrapin)
Cerrar los puertos/servicios que no esté utilizando o sean desconocidos, a fin de evitar que usuarios no autorizados exploten la información contenida en estos para lanzar ataques informáticos.	Critica	#9 Potential TCP Backdoor
Si no se utiliza, deshabilite el servicio expuesto; en caso contrario, asegúrese de utilizarlo exclusivamente en redes de gestión aisladas de la red corporativa.	Critica	#14 Intelligent Platform Management Interface (IPMI) Detected
Deshabilitar protocolos y servicios obsoletos y/o con vulnerabilidades conocidas.	Critica	#40 Windows SMB Version 1 (SMBv1) Detected
	Media	#164 EOL/Obsolete Software: SNMP Protocol Version Detected
Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, CBC, RC2, RC4, MD5, SHA1), en favor de protocolos criptográficamente más fuertes.	Alta	#62 SSL Server Supports Weak Encryption Vulnerability
	Alta	#107 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
	Media	#156 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
	Media	#157 Deprecated SSH Cryptographic Settings
	Media	#172 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)
	Media	#191 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)
	Media	#192 SSL Server Has SSLv2 Enabled Vulnerability
	Media	#209 X.509 Certificate SHA1 Signature Collision Vulnerability
	Media	#210 SSL Server Has SSLv3 Enabled Vulnerability
	Media	#257 Weak SSL/TLS Key Exchange
	Baja	#278 SHA1 deprecated setting for SSH
	Baja	#279 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)
Deshabilitar o restringir el acceso al servicio SNMP y modificar el community string utilizado por otro complejo o no conocido.	Alta	#104 Readable SNMP Information
	Alta	#131 Remote Management Service Accepting Unencrypted Credentials Detected (FTP)

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
Utilice los servicios alternativos que proporcionan cifrado, como SSH para reemplazar Telnet, FTPS o SFTP para reemplazar FTP y HTTPS con TLS para reemplazar HTTP	Media	#260 Web Server Uses Plain Text Basic Authentication
Aplicar el atributo “SECURE” a las cookies de sesión para asegurar su envío exclusivamente mediante comunicación cifrada.	Media	#148 Session Cookie Does Not Contain the "Secure" Attribute
Instalar un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.	Media	#153 SSL Certificate - Self-Signed Certificate
	Media	#159 SSL Certificate - Signature Verification Failed Vulnerability
Instalar un certificado que no exceda la validez máxima recomendada acorde a las buenas prácticas de seguridad.	Media	#154 SSL Certificate - Invalid Maximum Validity Date Detected
Instalar un certificado de servidor con fechas de inicio y final válidas.	Media	#155 SSL Certificate - Expired
Asegurar que todas las reglas de filtrado del firewall son correctas y suficientemente estrictas.	Media	#170 Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure
	Media	#251 UDP Source Port Pass Firewall
En lo posible, no publicar hacia Internet interfaces de gestión (por ejemplo SSH) y utilizar una VPN para acceder a las mismas.	Media	#171 Encrypted Management Interfaces Accessible On Cisco Device
Configurar los servicios utilizados de acuerdo a las buenas prácticas y recomendaciones de seguridad indicadas por los fabricantes.	Media	#174 SMBv2 Signing Not Required
	Media	#220 Account Brute Force Possible Through IIS NTLM Authentication Scheme
	Media	#252 Web Directories Listable Vulnerability
	Media	#271 NetBIOS Shared Folder List Available
	Baja	#288 NTP Information Disclosure Vulnerability
Utilizar HTTPS en lugar de HTTP para todos los servicios web expuestos, sobre todo en páginas de inicio de sesión o que transmiten información sensible.	Media	#196 Web Server Uses Plain-Text Form Based Authentication
Utilizar claves públicas de longitudes consideradas seguras (mínimo 2048 bits)	Media	#203 SSH Server Public Key Too Small
	Media	#212 Deprecated Public Key Length
Deshabilitar el acceso a los protocolos obsoletos SNMPv1 y SNMPv2.	Media	#208 SNMP GETBULK Reflected Distributed Denial-of-Service Vulnerability
Configurar el servidor web para utilizar todos los encabezados de seguridad HTTP acordes a las buenas prácticas de seguridad.	Media	#211 HTTP Security Header Not Detected

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
En lo posible, no activar el modo de depuración (DEBUG) en plataformas utilizadas en ambientes productivos.	Media	#221 ASP.NET DEBUG Method Enabled Security Issue
Aplicar y/o configurar correctamente los atributos necesarios	Baja	#286 AutoComplete Attribute Not Disabled for Password in Form Based Authentication

Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta :** La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red :** Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad :** Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades :** Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares :** Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.

En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

Etapa 1: Reconocimiento y Enumeración

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para determinar la superficie de ataque.

Etapa 2: Detección de Vulnerabilidades

Se utilizaron herramientas automatizadas para identificar y evaluar vulnerabilidades en los sistemas auditados. Este proceso puede incluir análisis de código, escaneo de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.
A continuación se listan algunos de los elementos buscados, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.

Etapa 3: Análisis de Resultados

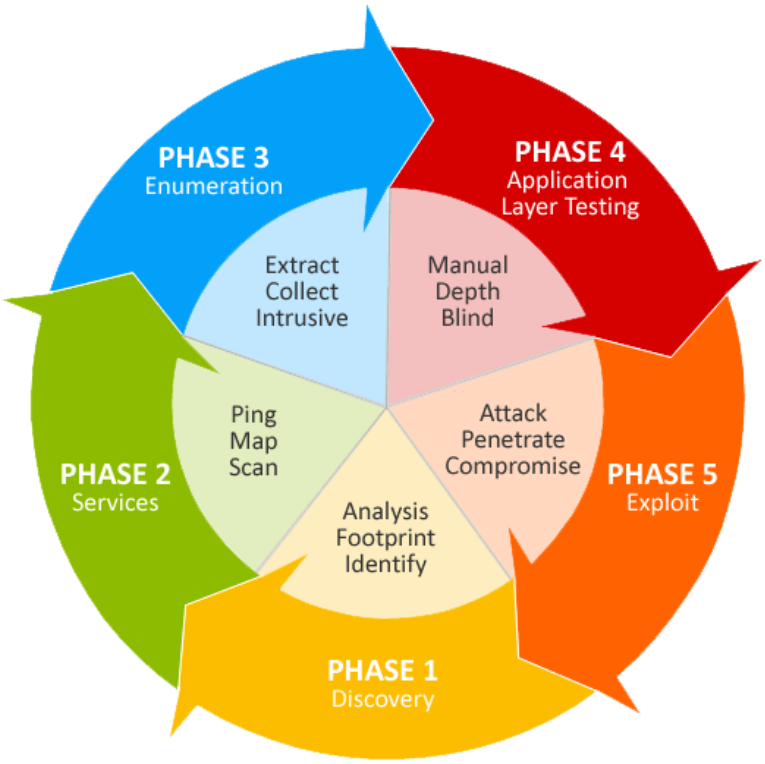
Se realizó un análisis de los resultados provistos por la herramienta de escaneo, con el objetivo de depurar hallazgos repetidos y descartar falsos positivos evidentes. De acuerdo al tiempo disponible para las tareas, el análisis se limitó a la interpretación y correlación de las detecciones automáticas.

Etapa 4: Informes

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, destacando el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información asociada necesaria para su identificación y corrección.

Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.



OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Si bien se trata de un proceso mayoritariamente manual, durante el análisis se utilizaron una serie de herramientas automatizadas que permitieron disminuir los tiempos necesarios para la finalización de las tareas, como así también permitieron la manipulación del tráfico enviado a los servicios analizados.