Executive Vulnerability Report

This report contains sensitive information. Unauthorized distribution is prohibited.

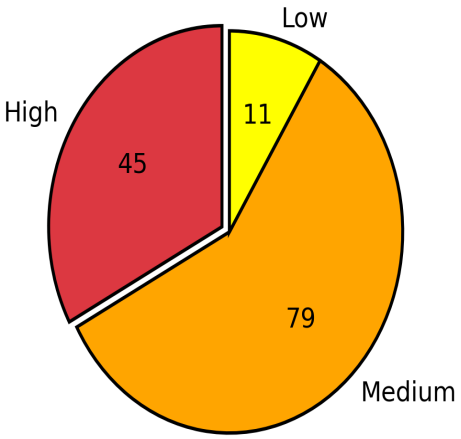
Created by: Greenbone Vulnerability Manager

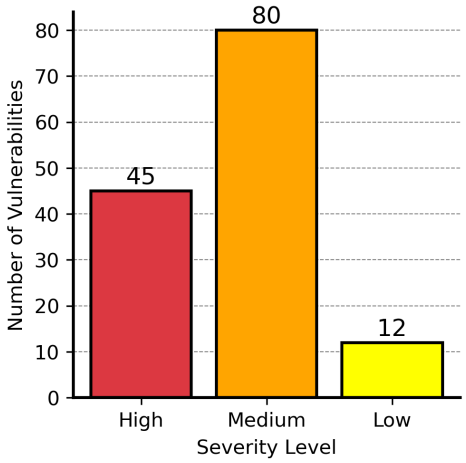
Date: 2024-08-27

1. Executive Summary

The purpose of this vulnerability scan was to identify weaknesses within our IT infrastructure that could be exploited by attackers, potentially leading to financial loss, regulatory penalties, or damage to our reputation. Of the 2 hosts scanned, 137 vulnerabilities were found, with 45 categorized as high, posing the most significant risk. Immediate remediation of any high vulnerabilities identified is necessary to avoid potential business disruptions and ensure the continued trust of our customers. The report provides detailed findings and actionable recommendations to mitigate these risks, safeguarding our operations.

2. Key Findings





Vulnerability Severity	Count
High	45
Medium	80
Low	12

3. Top 10 Vulnerabilities

Vulnerability	CVSS	Impact	Remediation
Possible Backdoor: Ingreslock	10.0	Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.	A whole cleanup of the infected system is recommended.
Operating System (OS) End of Life (EOL) Detection	10.0	An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
rlogin Passwordless Login	10.0	This vulnerability allows an attacker to gain complete control over the target system.	Disable the rlogin service and use alternatives like SSH instead.
TWiki XSS and Command Execution Vulnerabilities	10.0	Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.	Upgrade to version 4.2.4 or later.
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0	By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.	Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

4. Recommendations

Immediately address any critical vulnerabilities, continue to perform regular security assessments, and allocate resources to strengthen the security posture of our organization.

5. Conclusion

Addressing these vulnerabilities will help mitigate significant risks to the organization and ensure compliance with industry standards. We recommend taking immediate action on any critical vulnerabilities and

implementing long-term strategies to improve our security framework.

Appendix: Definitions

Term	Definition
CVE (Common Vulnerabilities and Exposure)	A list of publicly disclosed computer security flaws, each identified by a unique number called a CVE ID.
Severity	The level of impact that a vulnerability could have on the organisation, categorised as High, Medium, or Low with high being the most critical, etc.
Exploit	A piece of code or technique that takes advantage of a vulnerability to compromise a system.
Vulnerability	A weakness in a system that can be exploited by an attacker to perform malicious actions.
Vulnerability Scan	Automated process that identifies, evaluates, and reports potential security weaknesses in an organisation's IT systems.

Appendix: Recommended Actions to be Taken Based on Vulnerability Severity

Severity	Description	Recommended Actions
High	Vulnerabilities that pose an immediate threat to the organisation and could lead to significant business impact if exploited.	1. Immediate remediation within 24 hours. 2. Apply security patches or mitigations. 3. Increase monitoring on affected systems. 4. Notify relevant stakeholders.
Medium	Vulnerabilities that have a moderate impact and could lead to significant issues if left unaddressed.	1. Remediate within 7 days. 2. Apply available patches or mitigations. 3. Monitor for signs of exploitation.
Low	Vulnerabilities that have a minor impact and are less likely to be exploited but should still be addressed.	1. Remediate within 30 days. 2. Apply patches as part of regular maintenance. 3. Monitor the situation to ensure no escalation.

Appendix: Detailed Vulnerability List

IP Address	Severity	Summary	Solution
192.168.100.6	Medium	Reports if the remote FTP Server allows anonymous logins.	If you do not want to share files, you should disable anonymous logins.
192.168.100.28	Medium	Reports if the remote FTP Server allows anonymous logins.	If you do not want to share files, you should disable anonymous logins.
192.168.100.28	Medium	Apache HTTP Server is prone to a cookie information disclosure vulnerability.	Update to Apache HTTP Server version 2.2.22 or later.
192.168.100.6	Medium	Apache HTTP Server is prone to a cookie information disclosure vulnerability.	Update to Apache HTTP Server version 2.2.22 or later.
192.168.100.28	High	Apache Tomcat is prone to a remote code execution (RCE) vulnerability (dubbed 'Ghostcat') in the AJP connector.	Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.
192.168.100.6	High	Apache Tomcat is prone to a remote code execution (RCE) vulnerability (dubbed 'Ghostcat') in the AJP connector.	Update Apache Tomcat to version 7.0.100, 8.5.51, 9.0.31 or later. For other products using Tomcat please contact the vendor for more information on fixed versions.
192.168.100.28	Medium	awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
192.168.100.6	Medium	awiki is prone to multiple local file include (LFI) vulnerabilities because it fails to properly sanitize user-supplied input.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

192.168.100.6	Medium	The Mailserver on this host answers to VRFY and/or EXPN requests.	Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
192.168.100.28	Medium	The Mailserver on this host answers to VRFY and/or EXPN requests.	Disable VRFY and/or EXPN on your Mailserver. For postfix add 'disable_vrfy_command=yes' in 'main.cf'. For Sendmail add the option 'O PrivacyOptions=goaway'. It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.
192.168.100.6	Medium	The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
192.168.100.28	Medium	The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.	Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
192.168.100.28	High	DistCC is prone to a remote code execution (RCE) vulnerability.	Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.
192.168.100.6	High	DistCC is prone to a remote code execution (RCE) vulnerability.	Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.

192.168.100.28	High	Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.	Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
192.168.100.6	High	Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.	Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts
192.168.100.28	Medium	The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.	Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: AllowOverride None order deny, allow deny from all allow from localhost
192.168.100.6	Medium	The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.	Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf: AllowOverride None order deny, allow deny from all allow from localhost
192.168.100.28	High	It was possible to login into the remote FTP server using weak/known credentials.	Change the password as soon as possible.
192.168.100.6	High	It was possible to login into the remote FTP server using weak/known credentials.	Change the password as soon as possible.
192.168.100.28	High	It was possible to login into the remote FTP server using weak/known credentials.	Change the password as soon as possible.
192.168.100.6	High	It was possible to login into the remote FTP server using weak/known credentials.	Change the password as soon as possible.

192.168.100.6	Medium	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
192.168.100.6	Medium	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
192.168.100.28	Medium	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
192.168.100.28	Medium	The remote host is running a FTP service that allows cleartext logins over unencrypted connections.	Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.
192.168.100.28	Medium	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.	Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
192.168.100.6	Medium	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.	Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.
192.168.100.28	Low	The remote host responded to an ICMP timestamp request.	Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)
192.168.100.6	Low	The remote host responded to an ICMP timestamp request.	Various mitigations are possible: - Disable the support for ICMP timestamp on the remote host completely - Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

192.168.100.28	High	Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code (remote code execution/RCE) on a targeted system with elevated privileges.	Disable class-loading. Please contact the vendor of the affected system for additional guidance.
192.168.100.6	Medium	jQuery is prone to a cross-site scripting (XSS) vulnerability.	Update to version 1.6.3 or later.
192.168.100.28	Medium	jQuery is prone to a cross-site scripting (XSS) vulnerability.	Update to version 1.6.3 or later.
192.168.100.28	Medium	jQuery is prone to a cross-site scripting (XSS) vulnerability.	Update to version 1.9.0 or later.
192.168.100.6	Medium	jQuery is prone to a cross-site scripting (XSS) vulnerability.	Update to version 1.9.0 or later.
192.168.100.28	Medium	Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.	Updates are available. Please see the references for more information.
192.168.100.6	Medium	Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.	Updates are available. Please see the references for more information.
192.168.100.28	High	It was possible to login into the remote MySQL as root using weak credentials.	'- Change the password as soon as possible - Contact the vendor for other possible fixes / updates
192.168.100.6	High	It was possible to login into the remote MySQL as root using weak credentials.	'- Change the password as soon as possible - Contact the vendor for other possible fixes / updates
192.168.100.28	High	The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
192.168.100.6	High	The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
192.168.100.6	High	PHP is prone to multiple vulnerabilities.	Update to version 5.3.13, 5.4.3 or later.
192.168.100.28	High	PHP is prone to multiple vulnerabilities.	Update to version 5.3.13, 5.4.3 or later.

192.168.100.6	Medium	Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.	Delete the listed files or restrict access to them.
192.168.100.28	Medium	Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.	Delete the listed files or restrict access to them.
192.168.100.28	Medium	phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
192.168.100.6	Medium	phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
192.168.100.28	High	A backdoor is installed on the remote host.	A whole cleanup of the infected system is recommended.
192.168.100.6	High	A backdoor is installed on the remote host.	A whole cleanup of the infected system is recommended.
192.168.100.28	High	It was possible to login into the remote PostgreSQL as user postgres using weak credentials.	Change the password as soon as possible.
192.168.100.6	High	It was possible to login into the remote PostgreSQL as user postgres using weak credentials.	Change the password as soon as possible.
192.168.100.6	Medium	The remote host is running QWikiwiki, a Wiki application written in PHP. The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

192.168.100.28	Medium	The remote host is running QWikiwiki, a Wiki application written in PHP. The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.	No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.
192.168.100.28	High	The rlogin service allows root access without a password.	Disable the rlogin service and use alternatives like SSH instead.
192.168.100.6	High	The rlogin service allows root access without a password.	Disable the rlogin service and use alternatives like SSH instead.
192.168.100.6	High	This remote host is running a rsh service.	Disable the rsh service and use alternatives like SSH instead.
192.168.100.28	High	This remote host is running a rsh service.	Disable the rsh service and use alternatives like SSH instead.
192.168.100.6	Medium	Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.	Updates are available. Please see the referenced vendor advisory.
192.168.100.28	Medium	Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.	Updates are available. Please see the referenced vendor advisory.
192.168.100.28	Medium	The remote server's SSL/TLS certificate has already expired.	Replace the SSL/TLS certificate by a new one.
192.168.100.6	Medium	The remote server's SSL/TLS certificate has already expired.	Replace the SSL/TLS certificate by a new one.
192.168.100.6	Medium	The remote server's SSL/TLS certificate has already expired.	Replace the SSL/TLS certificate by a new one.
192.168.100.28	Medium	The remote server's SSL/TLS certificate has already expired.	Replace the SSL/TLS certificate by a new one.
192.168.100.6	Medium	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

192.168.100.28	Medium	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
192.168.100.28	Medium	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
192.168.100.6	Medium	The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.	Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.
192.168.100.6	Medium	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.28	Medium	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.28	Medium	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.6	Medium	It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.28	Medium	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.6	Medium	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

192.168.100.28	Medium	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.6	Medium	It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.
192.168.100.6	Low	This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.	'- Remove support for 'DHE_EXPORT' cipher suites from the service - If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.
192.168.100.28	Low	This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.	'- Remove support for 'DHE_EXPORT' cipher suites from the service - If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.
192.168.100.6	Medium	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
192.168.100.28	Medium	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
192.168.100.28	Medium	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.
192.168.100.6	Medium	The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).	Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references). For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

192.168.100.6	High	OpenSSL is prone to security-bypass vulnerability.	Updates are available. Please see the references for more information.
192.168.100.28	High	OpenSSL is prone to security-bypass vulnerability.	Updates are available. Please see the references for more information.
192.168.100.28	Medium	The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
192.168.100.6	Medium	The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
192.168.100.6	Medium	The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
192.168.100.28	Medium	The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.	Users should contact their vendors for specific patch information. A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.
192.168.100.6	Medium	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.
192.168.100.28	Medium	This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.

192.168.100.28	Medium	This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.	'- Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.
192.168.100.6	Medium	This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.	'- Remove support for 'RSA_EXPORT' cipher suites from the service. - If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.
192.168.100.28	Medium	The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.	Replace the certificate with a stronger key and reissue the certificates it signed.
192.168.100.6	Medium	The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.	Replace the certificate with a stronger key and reissue the certificates it signed.
192.168.100.28	Medium	The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.	Replace the certificate with a stronger key and reissue the certificates it signed.
192.168.100.6	Medium	The remote SSL/TLS server certificate and/or any of the certificates in the certificate chain is using a RSA key with less than 2048 bits.	Replace the certificate with a stronger key and reissue the certificates it signed.
192.168.100.6	Low	This host is prone to an information disclosure vulnerability.	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
192.168.100.6	Low	This host is prone to an information disclosure vulnerability.	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
192.168.100.28	Low	This host is prone to an information disclosure vulnerability.	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

192.168.100.28	Low	This host is prone to an information disclosure vulnerability.	Possible Mitigations are: - Disable SSLv3 - Disable cipher suites supporting CBC cipher modes - Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+
192.168.100.28	Low	The remote host implements TCP timestamps and therefore allows to compute the uptime.	To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
192.168.100.6	Low	The remote host implements TCP timestamps and therefore allows to compute the uptime.	To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.
192.168.100.28	Medium	The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.	Replace Telnet with a protocol like SSH which supports encrypted connections.
192.168.100.6	Medium	The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.	Replace Telnet with a protocol like SSH which supports encrypted connections.
192.168.100.28	High	Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.	Use access restrictions to these dangerous HTTP methods or disable them completely.

192.168.100.6	High	Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE.	Use access restrictions to these dangerous HTTP methods or disable them completely.
192.168.100.28	High	This remote host is running a rexec service.	Disable the rexec service and use alternatives like SSH instead.
192.168.100.6	High	This remote host is running a rexec service.	Disable the rexec service and use alternatives like SSH instead.
192.168.100.6	High	This remote host is running a rlogin service.	Disable the rlogin service and use alternatives like SSH instead.
192.168.100.28	High	This remote host is running a rlogin service.	Disable the rlogin service and use alternatives like SSH instead.
192.168.100.28	Medium	bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.	Update to version 6.1.0 or later.
192.168.100.6	Medium	bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.	Update to version 6.1.0 or later.
192.168.100.28	Medium	TWiki is prone to a cross-site request forgery (CSRF) vulnerability.	Upgrade to TWiki version 4.3.2 or later.
192.168.100.6	Medium	TWiki is prone to a cross-site request forgery (CSRF) vulnerability.	Upgrade to TWiki version 4.3.2 or later.
192.168.100.6	Medium	TWiki is prone to a cross-site request forgery (CSRF) vulnerability.	Upgrade to version 4.3.1 or later.
192.168.100.28	Medium	TWiki is prone to a cross-site request forgery (CSRF) vulnerability.	Upgrade to version 4.3.1 or later.
192.168.100.6	High	TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.	Upgrade to version 4.2.4 or later.
192.168.100.28	High	TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.	Upgrade to version 4.2.4 or later.
192.168.100.6	High	UnrealIRCd is prone to authentication spoofing vulnerability.	Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.
192.168.100.28	High	UnrealIRCd is prone to authentication spoofing vulnerability.	Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

192.168.100.28	High	Detection of backdoor in UnrealIRCd.	Install latest version of unrealircd and check signatures of software you're installing.
192.168.100.6	High	Detection of backdoor in UnrealIRCd.	Install latest version of unrealircd and check signatures of software you're installing.
192.168.100.6	High	Try to log in with given passwords via VNC protocol.	Change the password to something hard to guess or enable password protection at all.
192.168.100.28	High	Try to log in with given passwords via VNC protocol.	Change the password to something hard to guess or enable password protection at all.
192.168.100.6	Medium	The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.	Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.
192.168.100.28	Medium	The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.	Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.
192.168.100.6	High	vsftpd is prone to a backdoor vulnerability.	The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
192.168.100.6	High	vsftpd is prone to a backdoor vulnerability.	The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
192.168.100.28	High	vsftpd is prone to a backdoor vulnerability.	The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
192.168.100.28	High	vsftpd is prone to a backdoor vulnerability.	The repaired package can be downloaded from the referenced vendor homepage. Please validate the package with its signature.
192.168.100.28	Medium	The remote SSH server is configured to allow / support weak encryption algorithm(s).	Disable the reported weak encryption algorithm(s).
192.168.100.6	Medium	The remote SSH server is configured to allow / support weak encryption algorithm(s).	Disable the reported weak encryption algorithm(s).

192.168.100.6	Medium	The remote SSH server is configured to allow / support weak host key algorithm(s).	Disable the reported weak host key algorithm(s).
192.168.100.28	Medium	The remote SSH server is configured to allow / support weak host key algorithm(s).	Disable the reported weak host key algorithm(s).
192.168.100.6	Medium	The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).	Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.
192.168.100.28	Medium	The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).	Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.
192.168.100.28	Low	The remote SSH server is configured to allow / support weak MAC algorithm(s).	Disable the reported weak MAC algorithm(s).
192.168.100.6	Low	The remote SSH server is configured to allow / support weak MAC algorithm(s).	Disable the reported weak MAC algorithm(s).