Internal Vulnerabilities by Issue - Alert

Issue 1: Trojan horses (CVSS: 10)
Summary: An unknown service runs on this port. It is sometimes opened by Trojan horses. Unless you know for sure what is behind it, you'd better check your system.
Solution: If a trojan horse is running, run a good antivirus scanner.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B)

Issue 2: Microsoft Windows Remote Desktop Services CVE-2019-0708 Remote Code Execution Vulnerability (BlueKeep) - (Remote Active) (CVSS: 10)
Summary: Microsoft Windows Remote Desktop Services is prone to the remote code execution vulnerability known as 'BlueKeep'.
Solution: The vendor has released updates. Please see the references for more information. As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2. NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.
Affected Nodes: Internal 10.200.1.15 (00:15:5D:01:07:24)

Issue 3: jQuery End of Life (EOL) Detection (Linux) (CVSS: 9.9)
Summary: The installed version of jQuery on the remote host has reached the End of Life (EOL) and should not be used anymore.
Solution: Update jQuery on the remote host to a still supported version.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 4: Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.30 or later. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 5: phpMyAdmin 4.5.0 <= 4.8.4 SQL Injection Vulnerability - PMASA-2019-2 (Linux) (CVSS: 9.8)
Summary: phpMyAdmin is prone to an SQL injection vulnerability.
Solution: Update to version 4.8.5.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 6: Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.

Solution: Update to version 2.4.53 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 7: Magento 2.3.x < 2.3.3 or 2.3.2-p1 Multiple Vulnerabilities - October 19 (CVSS: 9.8)
Summary: Magento is prone to multiple vulnerabilities, including remote code execution (RCE), and cross-site scripting (XSS). See the referenced advisories for further details on each specific vulnerability.
Solution: Update to version 2.3.2-p1, 2.3.3 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 8: Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.48 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 9: Magento Multiple Vulnerabilities (APSB20-22) (CVSS: 9.8)
Summary: Magento is prone to multiple vulnerabilities.
Solution: Update to version 1.9.4.5, 1.14.4.5, 2.3.4-p2 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 10: phpMyAdmin < 4.8.6 SQL Injection Vulnerability - PMASA-2019-3 (Linux) (CVSS: 9.8)
Summary: phpMyAdmin is prone to an SQL injection vulnerability.
Solution: Update to version 4.8.6 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 11: Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.49 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 12: Magento Multiple Vulnerabilities (APSB20-02) (CVSS: 9.8)
Summary: Magento is prone to multiple vulnerabilities.
Solution: Update to version 1.9.4.4, 1.14.4.4, 2.2.11, 2.3.4 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 13: Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (CVSS: 9.8)
Summary: Apache HTTP Server is prone to a buffer overflow vulnerability.
Solution: Update to version 2.4.52 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 14: Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (CVSS: 9.8)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 15: phpMyAdmin < 4.9.6, 5.x < 5.0.3 Multiple Vulnerabilities - PMASA-2020-5, PMASA-2020-6 (Linux) (CVSS: 9.8)
Summary: phpMyAdmin is prone to multiple vulnerabilities.
Solution: Update to version 4.9.6, 5.0.3 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 16: phpMyAdmin < 4.9.2 Multiple Vulnerabilities - PMASA-2019-5 (Linux) (CVSS: 9.8)
Summary: phpMyAdmin is prone to multiple vulnerabilities.
Solution: Update to version 4.9.2 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 17: Magento <= 2.3.5-p1 Multiple Vulnerabilities (APSB20-47) (CVSS: 9.6)
Summary: Magento is prone to multiple vulnerabilities.
Solution: Update to version 2.3.5-p2, 2.4.0 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 18: Apache HTTP Server mod_auth_digest Multiple Vulnerabilities (Linux) (CVSS: 9.1)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 19: Apache HTTP Server Memory Access Vulnerability (Linux) (CVSS: 9.1)
Summary: Apache HTTP Server is prone to a memory access vulnerability.
Solution: Update to version 2.4.41 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 20: Magento < 2.3.6, 2.4.x < 2.4.1 Multiple Vulnerabilities (APSB20-59) (CVSS: 9.1)
Summary: Magento is prone to multiple vulnerabilities.
Solution: Update to version 2.3.6, 2.4.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 21: phpMyAdmin < 4.9.4, 5.x < 5.0.1 SQL Injection Vulnerability - PMASA-2020-1 (Linux) (CVSS: 8.8)
Summary: phpMyAdmin is prone to an SQL injection vulnerability.
Solution: Update to version 4.9.4, 5.0.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 22: phpMyAdmin <= 5.1.1 CSV Injection Vulnerability - Linux (CVSS: 8.8)
Summary: phpMyAdmin is prone to a CSV injection vulnerability via Export Section.
Solution: 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.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 23: Magento 2.2.x < 2.2.10, 2.3.x < 2.3.3 or 2.3.2-p1 Multiple Vulnerabilities - October 19 (CVSS: 8.8)
Summary: Magento is prone to multiple vulnerabilities, including remote code execution (RCE), SQL injection, using components with known vulnerabilities, server-side request forgery (SSRF), arbitrary file deletion, XML external entity injection (XXE), cross-site scripting (XSS), information disclosure and others. See the referenced advisories for further details on each specific vulnerability.
Solution: Update to version 2.2.10, 2.3.3 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 24: Apache HTTP Server 2.4.7 - 2.4.51 Multiple Vulnerabilities - Linux (CVSS: 8.2)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.52 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 25: Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (CVSS: 8.1)
Summary: Apache HTTP Server is prone to a man-in-the-middle attack vulnerability.
Solution: Update to version 2.4.24, or 2.2.32, or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 26: phpMyAdmin < 4.9.5, 5.x < 5.0.2 Multiple SQL Injection Vulnerabilities - PMASA-2020-2, PMSA-2020-3, PMSA-2020-4 (Linux) (CVSS: 8)
Summary: phpMyAdmin is prone to multiple SQL injection vulnerabilities.
Solution: Update to version 4.9.5, 5.0.2 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 27: OpenSSH Privilege Escalation Vulnerability - May16 (CVSS: 7.8)
Summary: openssh is prone to a privilege escalation vulnerability.
Solution: Upgrade to OpenSSH version 7.2p2-3 or later.

Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 28: OpenSSH <= 8.6 Command Injection Vulnerability (CVSS: 7.8)
Summary: OpenSSH is prone to a remote code execution vulnerability.
Solution: 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.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 29: Apache HTTP Server < 2.4.39 Privilege Escalation Vulnerability (Linux) (CVSS: 7.8)
Summary: In Apache HTTP Server, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
Solution: Update to version 2.4.39 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 30: Apache HTTP Server mod_http2 Denial of Service Vulnerability (Linux) (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a denial of service vulnerability.
Solution: Apply the patch from the referenced advisory.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 31: Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (CVSS: 7.5)
Summary: In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
Solution: Update to version 2.4.38 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 32: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater) (CVSS: 7.5)
Summary: The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability.
Solution: '- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 33: phpMyAdmin < 4.9.10, 5.x < 5.1.3 Information Disclosure Vulnerability - Linux (CVSS: 7.5)
Summary: phpMyAdmin is prone to an information disclosure vulnerability.
Solution: Update to version 4.9.10, 5.1.3 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 34: Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (CVSS: 7.5)
Summary: Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed.
Solution: Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled competely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all statements within the webserver configuration needs to be verified for invalid HTTP methods.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 35: Apache HTTP Server Security Bypass Vulnerability - Jul16 (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a security bypass vulnerability.
Solution: Update to version 2.4.23 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 36: Apache HTTP Server 2.4.17 < 2.4.49 mod_proxy HTTP/2 Request Smuggling Vulnerability - Linux (CVSS: 7.5)
Summary: Apache HTTP Server is prone to an HTTP/2 request smuggling vulnerability in the 'mod_proxy' module.
Solution: Update to version 2.4.49 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 37: Apache HTTP Server Whitespace Defects Multiple Vulnerabilities (CVSS: 7.5)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 38: Apache HTTP Server mod_auth_digest DoS Vulnerability (Linux) (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a denial-of-service vulnerability.
Solution: Update to Apache HTTP Server 2.4.25 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 39: Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (CVSS: 7.5)

Summary: Apache HTTP Server is prone to a denial of service vulnerability.
Solution: Update to version 2.4.30 or later. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 40: Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a vulnerability in mod_session_crypto.
Solution: Update to version 2.4.25 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 41: Apache HTTP Server HTTP/2 connection DoS Vulnerability (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a denial-of-service vulnerability.
Solution: Update to Apache HTTP Server 2.4.34 or later. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 42: Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (CVSS: 7.5)
Summary: In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
Solution: Update to version 2.4.39 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 43: Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (CVSS: 7.5)
Summary: Apache HTTP Server is prone to a NULL pointer dereference vulnerability.
Solution: Update to version 2.4.48 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 44: OpenSSH Multiple Vulnerabilities Jan17 (Linux) (CVSS: 7.3)
Summary: openssh is prone to multiple vulnerabilities.
Solution: Upgrade to OpenSSH version 7.4 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 45: Magento 2.1.x < 2.1.18, 2.2.x < 2.2.9, 2.3.x < 2.3.2 Multiple Vulnerabilities - June 19 (CVSS: 7.2)
Summary: Magento is prone to multiple vulnerabilities, including remote code execution (RCE), cross-site scripting (XSS) and others. See the referenced advisories for further details on each specific vulnerability.
Solution: Update to version 2.1.18, 2.2.9, 2.3.2 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 46: OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability (CVSS: 7)
Summary: OpenSSH is prone to a privilege scalation vulnerability in certain configurations.
Solution: Update to version 8.8 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 47: phpMyAdmin Multiple Vulnerabilities -01 May16 (Linux) (CVSS: 6.8)
Summary: phpMyAdmin is prone to multiple vulnerabilities.
Solution: Upgrade to phpMyAdmin version 4.5.5.1 or later or apply the patch from the linked references.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 48: phpMyAdmin < 4.9.0 CSRF Vulnerability - PMASA-2019-4 (Linux) (CVSS: 6.5)
Summary: phpMyAdmin is prone to a CSRF vulnerability.
Solution: Update to version 4.9.0 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 49: Magento 2.x Multiple Vulnerabilities - March19 (CVSS: 6.5)
Summary: Magento 2.x is prone to multiple vulnerabilities.
Solution: Update to version 2.1.17, 2.2.8, 2.3.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 50: phpMyAdmin < 4.9.1 CSRF Vulnerability (Linux) (CVSS: 6.5)
Summary: phpMyAdmin is prone to a CSRF vulnerability.
Solution: Update to phpMyAdmin version 4.9.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 51: Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (CVSS: 6.1)
Summary: Apache HTTP Server is prone to a CRLF injection vulnerability.
Solution: Update to version 2.2.32, 2.4.25 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 52: phpMyAdmin 4.x < 4.8.4 Multiple Vulnerabilities - PMASA-2018-6, PMASA-2018-8 (Linux) (CVSS: 6.1)
Summary: phpMyAdmin is prone to multiple security vulnerabilities.
Solution: Update to version 4.8.4 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 53: phpMyAdmin Multiple XSS Vulnerabilities (PMASA-2016-11) - Linux (CVSS: 6.1)
Summary: phpMyAdmin is prone to multiple cross-site scripting (XSS) vulnerabilities.

Solution: Update to version 4.0.10.15, 4.4.15.5, or 4.5.5.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 54: phpMyAdmin Cross-Site Scripting Vulnerability (PMASA-2018-3)-Linux (CVSS: 6.1)
Summary: phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.
Solution: Upgrade to version 4.8.2 or newer. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 55: phpMyAdmin <= 4.8.2 XSS Vulnerability - PMASA-2018-5 (Linux) (CVSS: 6.1)
Summary: phpMyAdmin is prone to an authenticated Cross-Site Scripting (XSS) Vulnerability.
Solution: Update to version 4.8.3.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 56: Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (CVSS: 6.1)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.41 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 57: jQuery < 3.0.0 XSS Vulnerability (CVSS: 6.1)
Summary: jQuery is vulnerable to Cross-site Scripting (XSS) attacks.
Solution: Update to version 3.0.0 or later or apply the patch.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 58: jQuery < 3.4.0 Object Extensions Vulnerability (CVSS: 6.1)
Summary: jQuery is prone to multiple vulnerabilities regarding property injection in Object.prototype.
Solution: Update to version 3.4.0 or later. Patch diffs are available for older versions.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 59: Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (CVSS: 6.1)
Summary: Apache HTTP Server is prone to multiple vulnerabilities.
Solution: Update to version 2.4.42 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 60: jQuery 1.2 < 3.5.0 XSS Vulnerability (CVSS: 6.1)
Summary: jQuery is prone to a cross-site scripting (XSS) vulnerability in jQuery.htmlPrefilter and related methods.
Solution: Update to version 3.5.0 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 61: jQuery 1.0.3 < 3.5.0 XSS Vulnerability (CVSS: 6.1)
Summary: jQuery is prone to a cross-site scripting (XSS) vulnerability when appending HTML containing option elements.
Solution: Update to version 3.5.0 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 62: Apache HTTP Server Denial of Service Vulnerability Apr18 (Linux) (CVSS: 5.9)
Summary: Apache HTTP Server is prone to a denial of service vulnerability.
Solution: Update to version 2.4.30 or later. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 63: phpMyAdmin 4.0 <= 4.8.4 Arbitrary File Read Vulnerability - PMASA-2019-1 (Linux) (CVSS: 5.9)
Summary: phpMyAdmin is prone to an arbitrary file read vulnerability.
Solution: Update to version 4.8.5.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 64: Apache HTTP Server Denial of Service Vulnerability - Jul16 (CVSS: 5.9)
Summary: Apache HTTP Server is prone to a denial of service vulnerability.
Solution: Update to version 2.4.20 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 65: SSL/TLS: BREACH attack against HTTP compression (CVSS: 5.9)
Summary: SSL/TLS connections are vulnerable to the 'BREACH' (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack.
Solution: The following mitigation possibilities are available: 1. Disabling HTTP compression 2. Separating secrets from user input 3. Randomizing secrets per request 4. Masking secrets (effectively randomizing by XORing with a random secret per request) 5. Protecting vulnerable pages with CSRF 6. Length hiding (by adding random number of bytes to the responses) 7. Rate-limiting the requests Note: The mitigations are ordered by effectiveness (not by their practicality - as this may differ from one application to another).
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 66: Apache HTTP Server HTTP/2 SETTINGS Data Processing DoS Vulnerability (Linux) (CVSS: 5.9)
Summary: Apache HTTP Server is prone to a denial-of-service vulnerability.
Solution: Update to Apache HTTP Server 2.4.35 or later. Please see the references for more information.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 67: OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities (CVSS: 5.9)

Summary: OpenBSD OpenSSH is prone to multiple vulnerabilities.
Solution: Update to version 8.0 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 68: OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145) (CVSS: 5.9)
Summary: OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Solution: Update to version 8.5 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 69: phpMyAdmin Multiple XSS Vulnerabilities (PMASA-2016-12) - Linux (CVSS: 5.4)
Summary: phpMyAdmin is prone to multiple cross-site scripting (XSS) vulnerabilities.
Solution: Update to version 4.4.15.5, 4.5.5.1 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 70: Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (CVSS: 5.3)
Summary: Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrite.
Solution: Update to version 2.4.24 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 71: OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) (CVSS: 5.3)
Summary: OpenBSD OpenSSH is prone to an information disclosure vulnerability.
Solution: No known solution is available as of 16th November, 2021. Information regarding this issue will be updated once solution details are available. Note: This issue is not treated as a security issue by the vendor so no update might be provided in the future.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 72: Apache HTTP Server < 2.4.38 HTTP/2 DoS Vulnerability (Linux) (CVSS: 5.3)
Summary: By sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
Solution: Update to version 2.4.38 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 73: OpenSSH auth2-gss.c User Enumeration Vulnerability - Linux (CVSS: 5.3)
Summary: OpenSSH is prone to a user enumeration vulnerability.
Solution: 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.

Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 74: OpenSSH < 7.8 User Enumeration Vulnerability - Linux (CVSS: 5.3)
Summary: OpenSSH is prone to a user enumeration vulnerability.
Solution: Update to version 7.8 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 75: OpenSSH sftp-server Security Bypass Vulnerability (Linux) (CVSS: 5.3)
Summary: openssh is prone to a security bypass vulnerability.
Solution: Upgrade to OpenSSH version 7.6 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 76: Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (CVSS: 5.3)
Summary: Apache HTTP Server is prone to a tunneling misconfiguration vulnerability.
Solution: Update to version 2.4.48 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 77: Apache HTTP Server < 2.4.39 mod_http2 Use-After-Free Vulnerability (Linux) (CVSS: 5.3)
Summary: Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
Solution: Update to version 2.4.39 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 78: Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (CVSS: 5.3)
Summary: When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
Solution: Update to version 2.4.39 or later.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 79: SSL/TLS: Report Weak Cipher Suites (CVSS: 5)
Summary: 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.
Solution: 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.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13

(00:15:5D:01:07:1A)

Issue 80: Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (CVSS: 5)
Summary: The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.
Solution: '- DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.
Affected Nodes: Internal 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 81: Backup File Scanner (HTTP) - Unreliable Detection Reporting (CVSS: 5)
Summary: The script reports backup files left on the web server. Notes: - 'Unreliable Detection' means that a file was detected only based on a HTTP 200 (Found) status code reported by the remote web server when a file was requested. - As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.
Solution: Delete the backup files.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 82: Enabled Directory Listing Detection (CVSS: 5)
Summary: The script attempts to identify directories with an enabled directory listing.
Solution: If not needed disable the directory listing within the webservers config.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 83: Cleartext Transmission of Sensitive Information via HTTP (CVSS: 4.8)
Summary: The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.
Solution: 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.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 84: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (CVSS: 4.3)
Summary: It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.
Solution: 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.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 85: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (CVSS: 4)
Summary: The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).
Solution: 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.
Affected Nodes: Internal 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D)

Issue 86: Relative IP Identification number change (CVSS: 2.6)
Summary: The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.
Solution: Contact your vendor for a patch
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B)

Issue 87: TCP timestamps (CVSS: 2.6)
Summary: The remote host implements TCP timestamps and therefore allows to compute the uptime.
Solution: 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.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 88: WinRM Detection (CVSS: 0)
Summary: Windows Remote Management (WinRM) is running at this port. Windows Remote Management (WinRM) is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and operating systems, from different vendors, to interoperate.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 89: SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (CVSS: 0)
Summary: This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 90: SSL/TLS: Version Detection (CVSS: 0)
Summary: Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 91: OS Detection Consolidation and Reporting (CVSS: 0)
Summary: This script consolidates the OS information detected by several VTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional information which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community portal.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 92: DCE/RPC and MSRPC Services Enumeration (CVSS: 0)
Summary: Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. The actual reporting takes place in the NVT 'DCE/RPC and MSRPC Services Enumeration Reporting' (OID: 1.3.6.1.4.1.25623.1.0.10736)
Solution: Filter incoming traffic to this port.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 93: Unknown OS and Service Banner Reporting (CVSS: 0)
Summary: This NVT consolidates and reports the information collected by the following NVTs: - Collect banner of unknown services (OID: 1.3.6.1.4.1.25623.1.0.11154) - Service Detection (unknown) with nmap (OID: 1.3.6.1.4.1.25623.1.0.66286) - Service Detection (wrapped) with nmap (OID:

1.3.6.1.4.1.25623.1.0.108525) - OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937) If you know any of the information reported here, please send the full output to the referenced community portal.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 94: Hostname Determination Reporting (CVSS: 0)
Summary: The script reports information on how the hostname of the target was determined.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 95: HTTP Server Banner Enumeration (CVSS: 0)
Summary: This script tries to detect / enumerate different HTTP server banner (e.g. from a frontend, backend or proxy server) by sending various different HTTP requests (valid and invalid ones).
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 96: SMB/CIFS Server Detection (CVSS: 0)
Summary: This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 97: CGI Scanning Consolidation (CVSS: 0)
Summary: The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community portal.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 98: HTTP Security Headers Detection (CVSS: 0)
Summary: All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 99: SMBv1 enabled (Remote Check) (CVSS: 0)
Summary: The host has enabled SMBv1 for the SMB Server.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 100: Traceroute (CVSS: 0)
Summary: Collect information about the network route and network distance between the scanner host and the target host.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 101: SSL/TLS: Report Supported Cipher Suites (CVSS: 0)
Summary: This routine reports all SSL/TLS cipher suites accepted by a service. As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 102: SMB Remote Version Detection (CVSS: 0)
Summary: Detection of Server Message Block(SMB). This script sends SMB Negotiation request and try to get the version from the response.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 103: CPE Inventory (CVSS: 0)
Summary: This routine uses information collected by other routines about CPE identities of operating systems, services and applications detected during the scan. Note: Some CPEs for specific products might show up twice or more in the output. Background: After a product got renamed or a specific vendor was acquired by another one it might happen that a product gets a new CPE within the NVD CPE Dictionary but older entries are kept with the older CPE.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 104: Microsoft Internet Information Services (IIS) Detection (HTTP) (CVSS: 0)
Summary: HTTP based detection of Microsoft Internet Information Services (IIS).
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B)

Issue 105: SSL/TLS: Report Medium Cipher Suites (CVSS: 0)
Summary: This routine reports all Medium SSL/TLS cipher suites accepted by a service.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 106: Microsoft Remote Desktop Protocol (RDP) Detection (CVSS: 0)
Summary: A service supporting the Microsoft Remote Desktop Protocol (RDP) is running at this host.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 107: HTTP Server type and version (CVSS: 0)
Summary: This script detects and reports the HTTP Server's banner which might provide the type and version of it.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 108: ICMP Timestamp Detection (CVSS: 0)
Summary: The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could

theoretically be used to exploit weak time-based random number generators in other services.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D)

Issue 109: Services (CVSS: 0)
Summary: This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 110: SSL/TLS: Report Non Weak Cipher Suites (CVSS: 0)
Summary: This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.
Affected Nodes: Internal 10.200.1.16 (00:15:5D:01:07:1B), 10.200.1.15 (00:15:5D:01:07:24), 10.200.1.17 (00:15:5D:01:07:1D), 10.200.1.14 (00:15:5D:01:07:18), 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 111: DNS Server Detection (TCP) (CVSS: 0)
Summary: TCP based detection of a DNS server.
Affected Nodes: Internal 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 112: LDAP Detection (CVSS: 0)
Summary: A LDAP Server is running at this host. The Lightweight Directory Access Protocol, or LDAP is an application protocol for querying and modifying directory services running over TCP/IP.
Affected Nodes: Internal 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 113: SMB NativeLanMan (CVSS: 0)
Summary: It is possible to extract OS, domain and SMB server information from the Session Setup AndX Response packet which is generated during NTLM authentication.
Affected Nodes: Internal 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 114: Kerberos Detection (TCP) (CVSS: 0)
Summary: TCP based detection of a Kerberos server.
Affected Nodes: Internal 10.200.1.12 (00:15:5D:01:07:19), 10.200.1.13 (00:15:5D:01:07:1A)

Issue 115: SSH Server type and version (CVSS: 0)
Summary: This detects the SSH Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 116: robot(s).txt exists on the Web Server (CVSS: 0)
Summary: Web Servers can use a file called /robot(s).txt to ask search engines to ignore certain files and directories. By nature this file can not be used to protect private files from public read access.
Solution: Review the content of the /robot(s).txt file and consider removing the files from the server or protect them in other ways in case you actually intended non-public availability.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 117: SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (CVSS: 0)
Summary: The SSL/TLS certificate contains a common name (CN) that does not match the hostname.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 118: SSL/TLS: Collect and Report Certificate Details (CVSS: 0)
Summary: This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 119: Response Time / No 404 Error Code Check (CVSS: 0)
Summary: This VT tests if the remote web server does not reply with a 404 error code and checks if it is replying to the scanners requests in a reasonable amount of time.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 120: Magento Detection (HTTP) (CVSS: 0)
Summary: HTTP based detection of Magento.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 121: SSH Protocol Algorithms Supported (CVSS: 0)
Summary: This script detects which algorithms are supported by the remote SSH Service.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 122: SSL/TLS: HTTP Strict Transport Security (HSTS) Missing (CVSS: 0)
Summary: The remote web server is not enforcing HSTS.
Solution: Enable HSTS or add / configure the required directives correctly following the guides linked in the

references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 123: SSL/TLS: NPN / ALPN Extension and Protocol Support Detection (CVSS: 0)
Summary: This routine identifies services supporting the following extensions to TLS: - Application-Layer Protocol Negotiation (ALPN) - Next Protocol Negotiation (NPN). Based on the availability of this extensions the supported Network Protocols by this service are gathered and reported.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 124: SSL/TLS: HTTP Public Key Pinning (HPKP) Missing (CVSS: 0)
Summary: The remote web server is not enforcing HPKP. Note: Most major browsers have dropped / deprecated support for this header in 2020.
Solution: Enable HPKP or add / configure the required directives correctly following the guides linked in the references. Note: Some web servers are not sending headers on specific status codes by default. Please review your web server or application configuration to always send these headers on every response independently from the status code. - Apache: Use 'Header always set' instead of 'Header set'. - nginx: Append the 'always' keyword to each 'add_header' directive. For different applications or web severs please refer to the related documentation for a similar configuration possibility.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 125: OpenSSH Detection Consolidation (CVSS: 0)
Summary: Consolidation of OpenSSH detections.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 126: SSL/TLS: Hostname discovery from server certificate (CVSS: 0)
Summary: It was possible to discover an additional hostname of this server from its certificate Common or Subject Alt Name.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 127: Apache HTTP Server Detection Consolidation (CVSS: 0)
Summary: Consolidation of Apache HTTP Server detections.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 128: jQuery Detection Consolidation (CVSS: 0)
Summary: Consolidation of jQuery detections.

Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 129: Fingerprint web server with favicon.ico (CVSS: 0)
Summary: The remote web server contains a graphic image that is prone to information disclosure.
Solution: Remove the 'favicon.ico' file or create a custom one for your site.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 130: PHP Detection (HTTP) (CVSS: 0)
Summary: HTTP based detection of PHP.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 131: phpMyAdmin Detection (CVSS: 0)
Summary: Detection of phpMyAdmin. The script sends a connection request to the server and attempts to extract the version number from the reply.
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 132: SSH Protocol Versions Supported (CVSS: 0)
Summary: Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints from the service. The following versions are tried: 1.33, 1.5, 1.99 and 2.0
Affected Nodes: External jansensupply.com (45.33.32.49)

Issue 133: Check open ports (CVSS: 0)
Summary: This plugin checks if the port scanners did not kill a service.
Affected Nodes: Internal 10.200.1.13 (00:15:5D:01:07:1A)