Vertraulich

Erstellt von

Showcase GmbH

Auditbericht

Bericht erstellt für

Automatisierter Pentest von Vorlage Hacktor Template 1

Bericht vom

28.12.22 12:28:17 CET

Audit vom

05.06.22 16:00:26 CEST

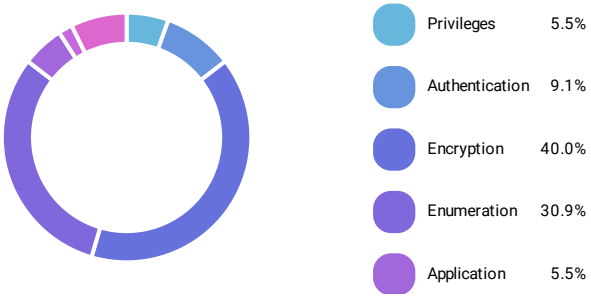
Beschreibung

Hacktor

ngs-hetzner-showcase-services

Zusammenfassung

Zusammenfassende Darstellung der Findings des Reports.



Dringlichkeit	Kategorie	Details
CRITICAL	CVEs	Kritische Sicherheitslücke Es wurden kritische Sicherheitslücken (CVE) detektiert. Die verwundbaren Systeme gefährden massiv den sicheren Betrieb der IT-Umgebung. **Empfehlung** Es sollte unmittelbar überprüft werden, ob alle verfügbaren Sicherheitspatches eingespielt wurden und gegebenenfalls Updates eingespielt werden. Sofern für veraltete Systeme keine Updates mehr erscheinen, sollte ein Umstieg auf einen aktuellen Service erwogen werden. Betroffen: 192.168.178.179, 192.168.178.22, 192.168.178.83
CRITICAL	Encryption	Unterstützt schwache SSL/TLS Chiffre (Algorithmus) SSL/TLS-Chiffren legen fest, mit welchen Verschlüsselungsalgorithmen Schlüssel getauscht werden und wie die Kommunikation abgesichert wird. Werden unsichere SSL/TLS-Chiffren angeboten, ist die hergestellte Verbindung nicht mehr sicher. **Empfehlung** Die Cipher Suite sollte aktualisiert und auf veraltete Verschlüsselungsalgorithmen verzichtet werden. Es muss sicher gestellt sein, dass ausschließlich aktuelle und sichere Technologien zum Einsatz kommen. Betroffen: 192.168.178.162:3389
CRITICAL	Privileges	Erlaubt Schreibzugriff Ein Schreibzugriff auf freigegebene Ordner, die nicht standardmäßig eingestellt sind, ist via SMB möglich. **Empfehlung** Es sollte geprüft werden, ob ein unauthentifizierter Schreibzugriff weiterhin bestehen soll oder nicht. Betroffen: 192.168.178.114:445
CRITICAL	Authentication	Erlaubt Gastzugriff Bei fehlerhaftem Login wird automatisch ein SMB Gastzugriff erteilt, der möglicherweise Zugriffsrechte besitzt.

Dringlichkeit	Kategorie	Details
		Empfehlung Der Zugriff auf SMB Shares sollte nur für authentifizierte Benutzer möglich sein und der Login über den Gast Accounts sollte deaktiviert werden. Betroffen: 192.168.178.114:445
CRITICAL	Authentication	Vorhandene SMB Network Shares Es existiert eine SMB Freigabe, die nicht unter die Standard-Freigaben fällt. **Empfehlung** Es sollte geprüft werden, ob die Freigaben berechtigterweise erstellt wurden. Betroffen: 192.168.178.114:445
CRITICAL	Authentication	Bruteforce HTTP Web Forms Für HTTP Web Forms werden eine oder mehrere unsichere Benutzer-Passwort-Kombinationen verwendet. **Empfehlung** Die Anmeldedaten sollten zügig nach den Kriterien für sichere Passwörter angepasst werden. Betroffen: 192.168.178.69:443
CRITICAL	Authentication	Bruteforce SMB Für SMB werden eine oder mehrere unsichere Benutzer-Passwort-Kombinationen verwendet oder ein Gastzugriff ist möglich. **Empfehlung** Die Anmeldedaten sollten zügig nach den Kriterien für sichere Passwörter angepasst werden. Betroffen: 192.168.178.114:445
CRITICAL	Privileges	Erlaubt Lesezugriff Ein Lesezugriff auf freigegebene Ordner ist via SMB möglich. **Empfehlung** Es sollte geprüft werden, ob ein unauthentifizierter Lesezugriff weiterhin bestehen soll oder nur über einen Benutzeraccount möglich sein soll. Betroffen: 192.168.178.114:445
HIGH	CVEs	Sicherheitslücken mit hohem Risiko Es wurden Sicherheitslücken (CVE) mit hohem Risiko detektiert. Die verwundbaren Systeme gefährden den sicheren Betrieb der IT-Umgebung.

Dringlichkeit	Kategorie	Details

Empfehlung
Es sollte unmittelbar überprüft werden, ob alle verfügbaren Sicherheitspatches eingespielt wurden und gegebenenfalls Updates eingespielt werden. Sofern für veraltete Systeme keine Updates mehr erscheinen, sollte ein Umstieg auf einen aktuellen Service erwogen werden.

Betroffen: 192.168.178.179

HIGH | Encryption

Anfällig für Sweet32 Attacken
Die Stream-Chiffre RC4 macht die Verbindung anfällig für Sweet32 Attacken.

Empfehlung
Die Chiffre, welche RC4 verwendet, sollte aus der Cipher Suite entfernt werden. Gegebenfalls sollte die gesamte Cipher Suite aktualisiert werden, um ausschließlich sichere und aktuelle Technologien zu nutzen.

Betroffen: 192.168.178.162:3389

HIGH | Encryption

Schwacher Diffie-Hellman Parameter
Ein schwacher Diffie-Hellman Parameter macht die den Schlüsseltausch anfällig für Attacken.

Empfehlung
Es muss sichergestellt werden, dass die Diffie-Hellman Primzahl pro Einsatzzweck individuell und ausreichend stark ist. Sie können eine entsprechende Diffie-Hellman Primzahl z.B. mit OpenSSL wie folgt erstellen: "openssl dhparam -out dhparam.pem 4096"

Betroffen: 192.168.178.22:443, 192.168.178.83:443

HIGH | Encryption

Unterstützt schwache SSL/TLS Chiffre (Parameter)
SSL/TLS-Chiffren legen fest, mit welchen Verschlüsselungsalgorithmen Schlüssel getauscht werden und wie die Kommunikation abgesichert wird. Werden unsichere SSL/TLS-Chiffren angeboten, ist die hergestellte Verbindung nicht mehr sicher.

Empfehlung
Die Cipher Suite sollte aktualisiert und auf veraltete Verschlüsselungsalgorithmen verzichtet werden. Es muss sicher gestellt sein, dass ausschließlich aktuelle und sichere Technologien zum Einsatz kommen.

Betroffen: 192.168.178.162:3389

HIGH | Privileges

Erlaubt Lesezugriff
Ein Lesezugriff auf Object Identifier (OID) ist via SNMP möglich.

Empfehlung
Es sollte geprüft werden, ob SNMP für diesen Host aktiviert sein muss und ob die OID Informationen schützenswert sind. Das SNMP Protokoll Version 3 unterstützt eine Authentifizierung mittels Benutzername und Kennwort.

Betroffen: 192.168.178.22:161, 192.168.178.83:161, 192.168.178.69:161

HIGH | Application

Anfällig für Shellshock

Dringlichkeit	Kategorie	Details
		Die Schwachstelle in der Unix-Shell Bash ermöglicht auf dem Zielsystem beliebige Befehle auszuführen und nichtautorisierten Zugriff zu erhalten. **Empfehlung** In aktuellen Versionen der Unix-Shell Bash wurde die Sicherheitslücke geschlossen. Die Schwachstelle lässt sich durch ein Update von Bash schließen. Betroffen: 192.168.178.114:5357, 192.168.178.1:5357, 192.168.178.44:5357
HIGH	Encryption	Anfällig nach Maßgabe der Datenschutzgrundverordnung (DSGVO) Die SSL/TLS-Verschlüsselung widerspricht dem aktuellen Stand der Technik und verstößt daher gegen Art. 32 DSVGO. **Empfehlung** Damit personenbezogene Daten zwischen dem Webserver und dem Besucher der Webseite sicher übertragen werden, müssen die eingesetzten SSL/TLS-Protokolle und Chiffren aktualisiert werden. Empfohlen ist ausschließlich der Einsatz von TLS 1.2 und TLS 1.3. und einer aktuellen Cipher Suite. Betroffen: 192.168.178.162:3389
HIGH	Encryption	Unterstützt schwache SSL/TLS Chiffre (Algorithmus) SSL/TLS-Chiffren legen fest, mit welchen Verschlüsselungsalgorithmen Schlüssel getauscht werden und wie die Kommunikation abgesichert wird. Werden unsichere SSL/TLS-Chiffren angeboten, ist die hergestellte Verbindung nicht mehr sicher. **Empfehlung** Die Cipher Suite sollte aktualisiert und auf veraltete Verschlüsselungsalgorithmen verzichtet werden. Es muss sicher gestellt sein, dass ausschließlich aktuelle und sichere Technologien zum Einsatz kommen. Betroffen: 192.168.178.162:3389
HIGH	Enumeration	Verwendet gewöhnlichen Community String Für SNMP werden eine oder mehrere Community Strings zur Nutzerauthentifizierung verwendet, die häufig verwendet werden und daher besonders unsicher sind. **Empfehlung** Falls möglich, sollte eine Umstellung auf SNMPv3 erfolgen, da ab dieser Version eine Authentifizierung mittels Benutzername und Kennwort zur Verfügung steht. Betroffen: 192.168.178.22:161, 192.168.178.83:161, 192.168.178.69:161
HIGH	Enumeration	Preisgabe von Betriebssystem (Deep Scan) Die Version des verwendeten Betriebssystems hilft Hackern bei der Auswahl geeigneter Angriffsvektoren. **Empfehlung** Der Zugriff auf diese OID sollte deaktiviert werden oder nur authentifizierten Benutzern möglich sein. Betroffen: 192.168.178.22:161, 192.168.178.83:161, 192.168.178.69:161
HIGH	Encryption	Anfällig für SLOTH Attacke

Dringlichkeit	Kategorie	Details
		Schwache Hashfunktionen (MD5, SHA-1) erlauben eine SLOTH (Security Losses from Obsolete and Truncated Transcript Hashes) Attacke. Betroffen: 192.168.178.162:3389
HIGH	Encryption	Anfällig für Logjam Attacken Indem eine Schwachstelle im Diffie-Hellman-Schlüsselaustausch ausgenutzt wird, kommen Angreifer an die geheimen Schlüssel. Betroffen: 192.168.178.22:443, 192.168.178.83:443
MEDIUM	CVEs	Sicherheitslücken mit mittlerem Risiko Es wurden Sicherheitslücken (CVE) mit mittlerem Risiko detektiert. Die verwundbaren Systeme können potenziell den sicheren Betrieb der IT-Umgebung gefährden. **Empfehlung** Es sollte überprüft werden, ob alle verfügbaren Sicherheitspatches eingespielt wurden und gegebenenfalls Updates eingespielt werden. Betroffen: 192.168.178.179, 192.168.178.22, 192.168.178.83
MEDIUM	Application	Fehlende HTTPS-Umleitung Wird die Adresse über HTTP aufgerufen, findet keine Weiterleitung auf HTTPS statt. **Empfehlung** Der Aufruf einer Webseite über HTTP sollte in der Regel unterbunden werden. Dazu müssen alle Anfragen über HTTP auf automatisch HTTPS umgeleitet werden. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.162:8080, 192.168.178.2:3128, 192.168.178.1:80, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:80, 192.168.178.25:8080, 192.168.178.44:80, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.69:631
MEDIUM	Encryption	Unterstützt SSH-Passwort-Authentifizierung Eine auf asymetrischen Schlüsseln basierende Authentifizierung gilt als sicherer denn über ein Passwort. **Empfehlung** Der SSH Zugriff sollte soweit möglich auf das Public-Key-Verfahren umgestellt und eine Authentifizierung via Kennwort deaktiviert werden. Bei Umstellung auf das Public-Key-Verfahren sollte auch das Key-Management geplant werden. Betroffen: 192.168.178.162:22, 192.168.178.179:22, 192.168.178.2:22, 192.168.178.20:22, 192.168.178.80:22, 192.168.178.81:22
MEDIUM	Authentication	Ermöglicht Zugriff auf Loginseite kritischer Systeme Die über HTTP erreichbare Seite beinhaltet die Loginmaske eines kritischen Systems. Betroffen: 192.168.178.1:80, 192.168.178.44:80
MEDIUM	Encryption	Unterstützt schwache SSL/TLS Handshake Parameter

Dringlichkeit	Kategorie	Details
		Bei der Erstellung und Verifikation von Signaturen während des TLS-Handshakes wird ein unsicherer Signaturalgorithmus und/oder eine unsichere Hashfunktion verwendet. **Empfehlung** Die Algorithmen für Signatur und Hashfunktion sollten angepasst werden. Für die Signatur sollte insbesondere DSA nicht mehr zum Einsatz kommen und stattdessen RSA oder ECDSA verwendet werden. Für die Hashfunktion sollten MD5 und SHA-1 deaktiviert und SHA-224/256/384/512 Verwendung finden. Betroffen: 192.168.178.162:3389, 192.168.178.179:443, 192.168.178.179:623, 192.168.178.179:5900, 192.168.178.1:443, 192.168.178.22:443, 192.168.178.44:443, 192.168.178.83:443, 192.168.178.69:443
MEDIUM	Privacy	Setzt Cookies ohne Zustimmung Obwohl der Nutzer kein Einverständnis gegeben hat, werden Cookies gespeichert. Dies ist nur für technisch notwendige Cookies erlaubt. **Empfehlung** Alle Cookies, die ohne Zustimmung gesetzt werden, sollten auf Ihre technische Notwendigkeit hin überprüft werden. Betroffen: 192.168.178.22:80, 192.168.178.22:443, 192.168.178.83:80, 192.168.178.83:443
MEDIUM	Enumeration	Öffentlich erreichbares Backend Das Backend ist öffentlich erreichbar. Schränke den Zugriff ein, z.B. mit einem VPN. Betroffen: 192.168.178.22:80, 192.168.178.22:443, 192.168.178.83:80, 192.168.178.83:443
MEDIUM	Encryption	Verwendet bekannte Diffie-Hellman Primzahl Die Verwendung einer unsicheren Diffie-Hellman Primzahl gefährdet die Perfect Forward Secrecy und somit die Verschlüsselung. **Empfehlung** Es muss sichergestellt werden, dass die Diffie-Hellman Primzahl pro Einsatzzweck individuell und ausreichend stark ist. Sie können eine entsprechende Diffie-Hellman Primzahl z.B. mit OpenSSL wie folgt erstellen: "openssl dhparam -out dhparam.pem 4096" Betroffen: 192.168.178.22:443, 192.168.178.83:443
MEDIUM	Encryption	Unsicheres SSL/TLS Protokoll (TLSv1) TLSv1 ist veraltet und wird als nicht mehr als sicher angesehen. **Empfehlung** TLSv1 sollte deaktiviert werden. Empfohlen ist ausschließlich der Einsatz von TLSv1.2 und TLSv1.3. Betroffen: 192.168.178.162:3389, 192.168.178.69:443
MEDIUM	Encryption	Unsichere Server-Host-Schlüsselalgorithmen Im Rahmen des SSH-Verbindungsaufbaus findet ein Schlüsselaustausch (Key Exchange) statt. Währenddessen einigen sich Client und Server auf einen gemeinsamen Verschlüsselungs-Schlüssel. Dabei sollte ein sicheres Verschlüsselungsverfahren gewählt werden.

Dringlichkeit	Kategorie	Details
		Betroffen: 192.168.178.162:22, 192.168.178.2:22, 192.168.178.20:22, 192.168.178.24:22, 192.168.178.25:22, 192.168.178.41:22, 192.168.178.80:22, 192.168.178.81:22
MEDIUM	Encryption	Unsichere Schlüsselaustausch-Algorithmen Im Rahmen des SSH-Verbindungsaufbaus findet ein Schlüsselaustausch (Key Exchange) statt. Der gemeinsame Sitzungsschlüssel wird für die Authentifizierung und Verschlüsselung der Sitzung genutzt. Wird eine unsichere Schlüsseltausch-Methode verwendet, ist die Absicherung der Verbindung gefährdet. Betroffen: 192.168.178.162:22, 192.168.178.179:22, 192.168.178.2:22, 192.168.178.20:22, 192.168.178.24:22, 192.168.178.25:22, 192.168.178.41:22, 192.168.178.80:22, 192.168.178.81:22
MEDIUM	Encryption	Anfällig nach Maßgabe des BSI (Bundesamt für Sicherheit in der Informationstechnik) Die SSL/TLS-Verschlüsselung entspricht nicht der Checkliste TR-03116-4. Betroffen: 192.168.178.162:3389, 192.168.178.179:443, 192.168.178.179:623, 192.168.178.179:5900, 192.168.178.2:8006, 192.168.178.1:443, 192.168.178.22:443, 192.168.178.44:443, 192.168.178.83:443, 192.168.178.69:443
MEDIUM	Encryption	Unterstützt RC4 Chiffren RC4 gilt nicht mehr als ausreichend sicher und sollte daher nicht verwendet werden. Betroffen: 192.168.178.162:3389
MEDIUM	Encryption	Unsichere Mac Algorithmen Der Message Authentication Code (MAC) dient dazu, Gewissheit über den Ursprung von Daten zu erhalten und sie auf Integrität zu überprüfen. Mittels Keyed-Hash Message Authentication Code (HMAC) wird diese Überprüfung abgesichert. Dabei sollte ein sicheres Verfahren zum Einsatz kommen. Betroffen: 192.168.178.162:22, 192.168.178.179:22, 192.168.178.2:22, 192.168.178.20:22, 192.168.178.24:22, 192.168.178.25:22, 192.168.178.41:22, 192.168.178.80:22, 192.168.178.81:22
MEDIUM	Encryption	Chiffre unterstützt MD5 MD5 gilt nicht mehr als ausreichend sicher und sollte daher nicht verwendet werden. Betroffen: 192.168.178.162:3389
MEDIUM	Enumeration	Preisgabe von Software (Deep Scan: Webanwendung) Mittels statistischer Verfahren konnten verwendete Technologien aufdeckt werden. Schränke die Möglichkeiten ein, Software (insbesondere Versionsnummern) von außen zu erkennen, um die Angriffsfläche zu verringen. **Empfehlung** Es muss sichergestellt werden, dass sämtliche nicht-relevante Informationen über verwendete Software, wie z.B. Name, Version, Author, etc. bereinigt wird, da diese dem Angreifer mehr Angriffsoberfläche bietet und ihm die Arbeit erleichtern. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.179:80, 192.168.178.179:443, 192.168.178.1:80, 192.168.178.1:443, 192.168.178.1:8181, 192.168.178.25:80, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:80, 192.168.178.44:443, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.92:80, 192.168.178.69:80, 192.168.178.69:443, 192.168.178.69:631

Dringlichkeit	Kategorie	Details
MEDIUM	Encryption	**Unterstützt client-initiierte SSL/TLS Renegotiation** Clients sollte es nicht erlaubt sein, eine Neuaushandlung der SSL/TLS-Verbindung zu initiieren. Diese Möglichkeit kann ausgenutzt werden, um den Server absichtlich zu überlasten und eine Denial of Service-Attacke (DoS) auszuführen. Betroffen: 192.168.178.179:623, 192.168.178.179:5900, 192.168.178.69:443
MEDIUM	Enumeration	**Fehlender Strict-Transport-Security Header** Die HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen, der sowohl vor Aushebelung der Verbindungsverschlüsselung als auch vor Session Hijacking schützt. **Empfehlung** Setze den HTTP Strict Transport Security (HSTS), um deine HTTPS-Verbindung abzusichern. Empfohlener Wert: max-age=31536000; includeSubDomains Betroffen: 192.168.178.22:80, 192.168.178.22:443, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.69:443
MEDIUM	Encryption	**Unsicheres SSL/TLS Protokoll (TLSv1.1)** TLSv1.1 ist veraltet und wird als nicht mehr als sicher angesehen. **Empfehlung** TLSv1.1 sollte deaktiviert werden. Empfohlen ist ausschließlich der Einsatz von TLSv1.2 und TLSv1.3. Betroffen: 192.168.178.162:3389, 192.168.178.69:443
LOW	CVEs	**Sicherheitslücken mit geringem Risiko** Es wurden Sicherheitslücken (CVE) mit niedrigem Risiko detektiert. Die verwundbaren Systeme können potenziell den sicheren Betrieb der IT-Umgebung gefährden. **Empfehlung** Es sollte überprüft werden, ob alle verfügbaren Sicherheitspatches eingespielt wurden und gegebenenfalls Updates eingespielt werden. Betroffen: 192.168.178.114, 192.168.178.179, 192.168.178.25, 192.168.178.22, 192.168.178.83
LOW	Enumeration	**Preisgabe von Hostnames über mDNS** Aktivierte Multicast DNS (mDNS) Funktionalitäten können missbraucht werden, um Informationen auszuspähen und Angriffe vorzubereiten. Prüfe, ob mDNS benötigt wird, deaktiviere ihn gegebenenfalls oder stelle sicher, dass er nur für vertrauenswürdige Clients erreichbar ist. Betroffen: 192.168.178.114, 192.168.178.69
LOW	Encryption	**Unterstützt nicht das neuste Protokoll (TLSv1.3)** Das neuste und sicherste Protokoll TLSv1.3 wird nicht unterstützt. **Empfehlung** TLSv1.3 sollte aktiviert werden. Empfohlen ist der Einsatz von TLSv1.2 und TLSv1.3. Betroffen: 192.168.178.162:3389, 192.168.178.179:443, 192.168.178.179:623, 192.168.178.179:5900, 192.168.178.22:443, 192.168.178.83:443, 192.168.178.69:443

Dringlichkeit	Kategorie	Details
LOW	Enumeration	Fehlender Content-Security-Policy Header Die HTTP Content-Security-Policy regelt welche Ressourcen in einer bestimmten Art und Weise im Browser geladen bzw. ausgeführt werden können. **Empfehlung** Es muss sichergestellt werden, dass der Content-Security-Policy Header in der Webanwendung oder im Proxy gesetzt ist. Der Content-Security-Policy Header ermöglicht es Webseiten, die Ressourcen zu steuern, die der Browser laden darf. Dies hilft beim Schutz vor Cross-Site-Scripting-Angriffen (XSS). Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.2:3128, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:80, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.92:80, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Preisgabe von Software (Basic Scan) Die Möglichkeit des Zugriffs auf Versionsnummern sollte eingeschränkt werden, um potentiellen Angreifern keine unnötigen Informationen zu liefern. **Empfehlung** Es muss sichergestellt werden, dass sämtliche nicht-relevante Informationen über verwendete Software, wie z.B. Name, Version, Author, etc. bereinigt werden, da diese dem Angreifer mehr Angriffsfläche bietet und ihm die Arbeit erleichtern. Betroffen: 192.168.178.162:22, 192.168.178.179:22, 192.168.178.179:49154, 192.168.178.2:22, 192.168.178.2:3128, 192.168.178.20:22, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.24:22, 192.168.178.25:22, 192.168.178.22:80, 192.168.178.22:161, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.80:22, 192.168.178.81:22, 192.168.178.83:80, 192.168.178.83:161, 192.168.178.69:161
LOW	Enumeration	Preisgabe von Software (Basic Scan: Headers) Der Server-Header beinhaltet Informationen über die Software, die von dem Ursprungsserver verwendet wurde. **Empfehlung** Es muss sichergestellt werden, dass sämtliche nicht-relevanten Informationen über verwendete Software, wie z.B. Name, Version, Author, etc. bereinigt werden. Diese bieten einem Angreifer mehr Angriffsoberfläche und erleichtern ihm die Arbeit. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.2:3128, 192.168.178.25:80, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Common Source Leak Dateien, die versteckt sein sollten, sind öffentlich zugänglich. **Empfehlung** Alle nicht notwendigen Webseitenressoucen dürfen für außenstehene nicht erreichbar sein. Sie könnten unter Umständen sensible Informationen enthalten, die dem Angreifer zusätzliche Angriffsoberfläche bietet. Betroffen: 192.168.178.179:80, 192.168.178.179:443
LOW	Enumeration	Fehlender X-Frame-Options Header

Dringlichkeit	Kategorie	Details
		Die X-Frame-Options können verwendet werden, um zu bestimmen, ob ein aufrufender Browser die Zielseite in einem <frame>, <iframe> oder <object> rendern also einbetten darf. **Empfehlung** Verhindere die Möglichkeit, die Zielseite in einem <frame>, <iframe> oder <object> einzubetten. Empfohlener Wert: DENY Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.2:3128, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:8080, 192.168.178.44:5357, 192.168.178.44:8181
LOW	Enumeration	Fehlender X-XSS-Protection Header Die X-XSS-Protection kann Browsern untersagen eine Zielseite zu laden, sofern eine Cross-Site Scripting (XSS) Attacke erkannt wird. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.2:3128, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Vermeidbarer X-Powered-By Header Viele Server sind in ihrer Standard Konfiguration sehr freizügig mit der Bekanntgabe von Informationen. Dies betrifft vor allem den X-Powered-By und Server-Header. Diese sollten aus Sicherheitsgründen immer deaktiviert werden. Betroffen: 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.25:8080
LOW	Encryption	Unterstützt schwache SSL/TLS Chiffre (Algorithmus) SSL/TLS-Chiffren legen fest, mit welchen Verschlüsselungsalgorithmen Schlüssel getauscht werden und wie die Kommunikation abgesichert wird. Werden unsichere SSL/TLS-Chiffren angeboten, ist die hergestellte Verbindung nicht mehr sicher. **Empfehlung** Die Cipher Suite sollte aktualisiert und auf veraltete Verschlüsselungsalgorithmen verzichtet werden. Es muss sicher gestellt sein, dass ausschließlich aktuelle und sichere Technologien zum Einsatz kommen. Betroffen: 192.168.178.162:3389, 192.168.178.179:443, 192.168.178.179:623, 192.168.178.179:5900, 192.168.178.2:8006, 192.168.178.1:443, 192.168.178.22:443, 192.168.178.44:443, 192.168.178.83:443, 192.168.178.69:443
LOW	Application	Ermöglicht ungültige Umleitung Die Webanwendung akzeptiert nicht vertrauenswürdige Eingaben. Das kann ein Angreifer nutzen, um auf eine nicht vertrauenswürdige URL weiterzuleiten. **Empfehlung** Inoffizielle oder nicht existente Anfragen müssen auf eine 404-Fehler umgeleitet werden, um sicherzustellen, dass Webseitenbesucher bei manipulierten Links sofort bemerken, dass hier was nicht stimmt. Betroffen: 192.168.178.114:4200
LOW	Enumeration	Fehlender Referrer-Policy Header Die Referrer-Policy stellt sicher, dass Referrer Informationen nur unter bestimmten Bedingungen gesendet werden dürfen.

Dringlichkeit	Kategorie	Details
		Empfehlung Es muss sichergestellt werden, dass der Referrer-Policy Header in der Webanwendung oder im Proxy gesetzt ist. Der HTTP-Header Referrer-Policy steuert, wie viele Referrer-Informationen in Anfragen enthalten sein sollen. Empfohlener Wert: strict-origin Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.179:80, 192.168.178.179:443, 192.168.178.2:3128, 192.168.178.1:80, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:80, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.92:80, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Fehlender X-Content-Type-Options Header Der einzige definierte Wert "nosniff" untersagt dem Internet Explorer durch MIME-Sniffing einen anderen als den deklarierten Inhaltstyp zu bestimmen und anzuwenden. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.2:3128, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Fehlender Feature-Policy Header Die Feature-Policy bestimmt, welche Funktionen oder APIs eines Browsers verwendet werden dürfen. Betroffen: 192.168.178.114:5357, 192.168.178.114:5985, 192.168.178.114:4200, 192.168.178.162:8080, 192.168.178.179:80, 192.168.178.179:443, 192.168.178.2:3128, 192.168.178.1:80, 192.168.178.1:5357, 192.168.178.1:8181, 192.168.178.25:8080, 192.168.178.22:80, 192.168.178.22:443, 192.168.178.44:80, 192.168.178.44:5357, 192.168.178.44:8181, 192.168.178.83:80, 192.168.178.83:443, 192.168.178.92:80, 192.168.178.69:443, 192.168.178.69:631
LOW	Enumeration	Erreichbarer Remote Control Service Dienste, über die eine Fernwartung durchgeführt werden können, sind aus Sicherheitsperspektive kritisch zu betrachten. Es sollte überprüft werden, ob der Service tatsächlich benötigt wird. Betroffen: 192.168.178.162:22, 192.168.178.162:3389, 192.168.178.179:22, 192.168.178.179:5900, 192.168.178.2:22, 192.168.178.20:22, 192.168.178.24:22, 192.168.178.25:22, 192.168.178.41:22, 192.168.178.80:22, 192.168.178.81:22

Disclaimer

Dieser Bericht wurde erstellt von

Showcase GmbH

im folgenden 'Autor' genannt.

Der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt. Alle Angebote sind freibleibend und unverbindlich. Der Autor behält es sich ausdrücklich vor, Teile der Seiten oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Dieser Bericht enthält vertrauliche und/oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind, oder dieser Bericht irrtümlich erhalten haben, informieren Sie bitte den Absender und löschen Sie diesen Bericht. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieses Berichtes und der darin enthaltenen Informationen sind nicht gestattet.