

Schutz für Ihre wichtigsten Ressourcen

Lehren aus „Operation Aurora“

McAfee Labs und McAfee Foundstone Professional Services

Inhaltsverzeichnis

Kurzfassung	3
Funktionsweise von Aurora	3
Lehren	4
Geistiges Eigentum	4
Software Configuration Management (SCM)	4
Offene Repositories mit geistigem Eigentum	5
Gegenmaßnahmen	11
Empfehlungen speziell für Perforce	12
McAfee-Schutz	14
Fazit	14
Mitwirkende und Danksagungen	15
Über McAfee Labs	15
Über McAfee Foundstone Professional Services	15
Über Perforce	15

Kurzfassung

„Operation Aurora“ zeigte ganz deutlich, dass die so genannten APTs (Advanced Persistent Threats) zur immer häufigeren Form komplexer und direkter Angriffe werden. Dabei verschaffen sich Angreifer mit heimtückischen Methoden Zugriff auf wichtige Systeme und halten diesen Zugriff so lange aufrecht, bis sie ihr Ziel erreicht haben. Für „Operation Aurora“ wurde eine APT-Technik eingesetzt, die sich hinsichtlich der Zielgruppe, des Ausnutzens, des Zugriffs und des Herausfilterns wertvollsten geistigen Eigentums der Opfer als äußerst erfolgreich erwies. Dieses Whitepaper beschreibt „Operation Aurora“, was wir daraus lernen können und wie wir uns in Zukunft erfolgreich vor solchen Angriffen schützen können.

Funktionsweise von Aurora

„Operation Aurora“ bestand aus zahlreichen Schritten, die aus Sicht der Benutzer alle unbemerkt und in Sekundenschnelle vonstatten gingen. Wie Sie in der Abbildung unten erkennen können, vollzog „Operation Aurora“ ihren Angriff in sechs einfachen Schritten, ohne dass es klare Anzeichen für böswillige Absichten oder Taten gegeben hätte:

1. Ein ins Ziel geratener Benutzer bekam aus „vertrauenswürdiger“ Quelle einen Link in einer E-Mail oder in einer Sofortnachricht.
2. Der Benutzer klickte den Link an und gelangte so auf eine Webseite in Taiwan, die Schadcode in Form von schädlichem JavaScript-Payload enthielt.
3. Dieses schädliche JavaScript enthielt ein Zero-Day-Exploit für Internet Explorer und wurde vom Browser des Benutzers heruntergeladen und ausgeführt.
4. Der Exploit lud dann von Servern in Taiwan einen als Bild getarnten Binärcode herunter und führte den schädlichen Payload aus.
5. Der Payload richtete eine Backdoor ein und verband sich mit einem Botnet in Taiwan.
6. Damit hatten die Angreifer vollen Zugriff auf die internen Systeme. Sie hatten es auf geistiges Eigentum und Systeme zum Software-Konfigurations-Management (Software Configuration Management, SCM) abgesehen, auf die sie nun durch die gefährdeten Systeme Zugriff hatten. Das kompromittierte System ließ sich zudem so manipulieren, dass die Angreifer noch weiter in das Netzwerk vordringen konnten.

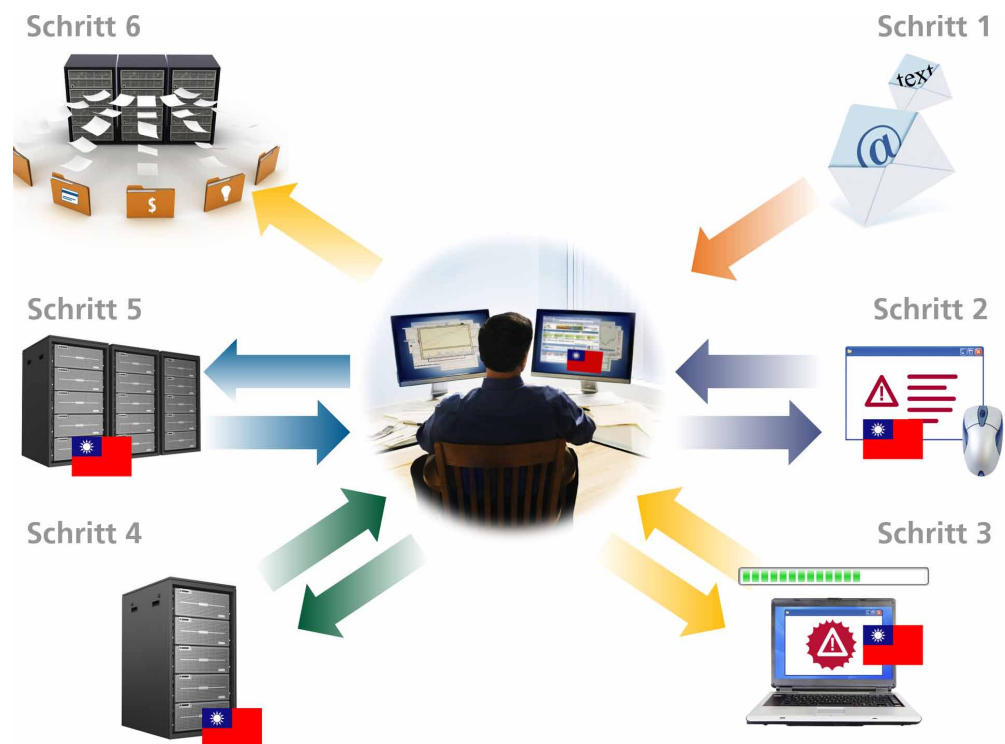


Abbildung 1: Die einzelnen Schritte beim Angriff „Operation Aurora“

Lehren

Direkte und zielgerichtete Angriffe wie „Operation Aurora“ sind generell nichts Neues. Zahlreiche Angriffe in den vergangenen Jahren beweisen, dass Angreifer berechnend sowie geduldig vorgehen und vor nichts zurückschrecken, um ihre Ziele zu erreichen – besonders, wenn es um den Diebstahl vertraulicher Daten geht. Doch während sich Regierung, Militär und Militärindustrie schon lange mit diesen Bedrohungen beschäftigen müssen, blieben die nun im Rahmen von „Operation Aurora“ angegriffenen kommerziellen Einrichtungen davon bislang verschont. Das gilt nun nicht mehr.

Geistiges Eigentum

In heutigen globalen Unternehmen gibt es zahlreiche Quellen geistigen Eigentums: Betriebsgeheimnisse, proprietäre Formeln, Urheberrechte, Marken und Quellcodes sind nur einige davon. Zu sagen, diese Quellen geistigen Eigentums seien die Kernwerte von Unternehmen auf der ganzen Welt, ist dabei noch untertrieben. Wenn diese Quellen geistigen Eigentums kompromittiert werden, stellt dies eine Bedrohung für Marktwirtschaft und Handel mit globalem Ausmaß dar.

Geistiges Eigentum wird in vielen verschiedenen Datenformaten gespeichert. Dazu gehören SCM-Systeme wie Perforce und IBM Rational-Software ebenso wie Dokument- und Content-Management-Systeme wie Microsoft SharePoint und EMC Documentum. Unsere Erfahrung bei der Beseitigung der Schäden in betroffenen Unternehmen warf ein neues Licht auf das Ziel von Hackerattacken: Repositories für geistiges Eigentum. Zum Schutz unserer Kunden und der Welt als solches beauftragten wir unsere besten Leute damit, diese Systeme unter die Lupe zu nehmen und etwaige Sicherheitslücken und Schwächen zu finden, die die Ausnutzung erleichtern. In den kommenden Monaten werden wir uns diesem immer beliebter werdenden Angriffsziel in aller Ausführlichkeit widmen und zuverlässige Gegenmaßnahmen für diese neu aufkommende Bedrohung anbieten.

Software Configuration Management (SCM)

In großen Unternehmen befindet sich Quellcode in der Regel in so genannten „Source-Strukturen“ von Quellcode-Kontrollsystemen. Diese Systeme werden als Software Configuration Management (SCM) bezeichnet. Zu den Anbietern solcher SCM-Systeme gehören unter anderem Perforce, Concurrent Versions System (CVS), Microsoft Visual SourceSafe (VSS) und IBM Rational. Unserer Erfahrung nach verfügt ein Großteil dieser Systeme über keinen Standardschutz. In der Regel ist es vielmehr Sache des Kunden, das System gegen Angreifer abzusichern, die die Standardkontrolle umgehen wollen. Worin also besteht die Bedrohung für solch ein System?

- *Im Diebstahl des geistigen Eigentums eines Unternehmens durch Herunterladen der gesamten Struktur, die dann aus dem Netzwerk des Unternehmens herausgezogen wird:* Diese Gefahr liegt auf der Hand, da es sich um konkreten und handfesten Diebstahl geistigen Eigentums handelt, das (wie bereits erwähnt) in der Technologiebranche oftmals unersetzlich ist.
- *In der Möglichkeit sowohl für befugte als auch für unbefugte Benutzer, Änderungen am Quellcode vorzunehmen:* Dieses Risiko spielt eine besonders große Rolle, da es dem Angreifer ermöglicht, unbemerkt Änderungen am Quellcode vorzunehmen und sich so in die Herstellungsprozesse einzuschleichen.
- *In der Verwendung des erbeuteten Quellcodes zum Aufspüren weiterer Lücken in den betroffenen Produkten:* Der Quellcode ist praktisch die Blaupause einer Software. Wenn Angreifer Zugriff auf einen solchen Bauplan haben, werden neue Angriffe auf ein Produkt vereinfacht. Dies ist ein besonderer Fall von Diebstahl geistigen Eigentums, der Kunden der betroffenen Produkte zusätzlichen Risiken aussetzt.

Durch unzureichende Sicherheitsmechanismen von der Stange – im Zusammenspiel mit der Tatsache, dass Unternehmen ihre SCM-Systeme nicht eigens abriegeln – haben Angreifer ungehinderten Zugang zu diesen Systemen. Mehr noch: Angesichts fehlender oder sprichwörtlich lückenhafter Sicherheitskontrollen ist es oft sogar ein Kinderspiel, Zugriff zu erhalten. Zudem sind die Protokolle der meisten SCM-Systeme nicht detailliert genug, um bei Nachforschungen bzw. Systemwiederherstellungen nach einem Angriff hilfreich zu sein.

Was aber hat all das mit „Operation Aurora“ zu tun? Im Laufe unserer Ermittlungen deckten wir in einer ganzen Reihe von Quellcode-Verwaltungssystemen Konzeptions- und Umsetzungsmängel auf, durch die Internetangriffe sehr Erfolg versprechend sind.

Dank der offenen Gestaltung der meisten aktuellen SCM-Systeme kann zudem viel von dem Quellcode, den die Systeme eigentlich schützen sollen, auf das Endgerätesystem des Entwicklers kopiert und dort verwaltet werden. Dass Entwickler Quellcode-Dateien auf ihre lokalen Systeme kopieren, sie dort bearbeiten und dann wieder in die Quellcode-Struktur einpflegen, ist nicht unüblich. Daher finden sich auf Endgeräten wie den von Entwicklern oder der Qualitätssicherung genutzten Systemen oft viele Codedateien. Für Angreifer bedeutet das: Sie müssen sich häufig gar nicht in die eventuell doch

abgesicherten SCM-Systeme hacken. Statt dessen nehmen sie lieber die jeweiligen Entwicklersysteme ins Visier, weil sie dort rasch große Mengen Quellcode ausspähen können.

Offene Repositories mit geistigem Eigentum

Wir möchten unsere Kunden und kommerzielle Unternehmen weltweit in die Lage versetzen, ihre Quellen geistigen Eigentums zu schützen. Die nun folgende Analyse (die sicher nicht allumfassend ist) kann daher als erste Welle von vielen betrachtet werden, die von McAfee® Labs™ ausgehen werden und die Sicherheit der beliebtesten Systeme für geistiges Eigentum zum Thema haben. In diesem Whitepaper betrachten wir Perforce auf Microsoft Windows-Systemen eingehender.

Das Unternehmen Perforce ist im kalifornischen Alameda ansässig und seit langem auf dem Gebiet der Quellcode-Kontrollsysteme führend. Die Zahl der Kunden (<http://www.perforce.com/perforce/customers/byname.html>) geht in die Tausende. Perforce-Produkte kommen bei den größten Unternehmen der Fortune 1000 zum Einsatz. Wir führten eine Sicherheitsprüfung von Perforce durch und stießen dabei auf Bemerkenswertes.

Fakt P-1: Der Perforce-Serverdienst (p4s.exe) wird mit Rechten auf Systemebene installiert

In der IT-Sicherheit wird jedoch üblicherweise empfohlen, allen Funktionen nur so wenig Rechte wie möglich einzuräumen. Entsprechend sollte Software generell nur als eingeschränkter Benutzer installiert werden. Die Software von Perforce wird jedoch unter Windows als „Systemdienst“ ausgeführt. Damit kann Malware in Prozesse auf Systemebene eingreifen und hat so Zugang zu allen administrativen Funktionen auf dem System.

In der Perforce-Dokumentation für UNIX werden die Leserinnen und Leser angewiesen, den Serverdienst ausdrücklich nicht als Root-Konto auszuführen. Eine vergleichbare Empfehlung für Windows gibt es hingegen nicht. Dadurch wird die Standardinstallation als lokales System ausgeführt, was einer Ausführung als Root-Konto unter Windows gleichkommt.

Fakt P-2: Nicht authentifiziertes Anlegen von Benutzern

In der Grundeinstellung ist es nicht authentifizierten, anonymen Benutzern möglich, neue Benutzer im Perforce-Depot anzulegen. Zudem wird zum Anlegen eines Benutzers kein Kennwort verlangt.

Fakt P-3: Kennwörter sind nicht verschlüsselt

Bei der Installation übermittelt Perforce viele Kennwörter standardmäßig als Klartext – insbesondere, wenn mit dem Perforce Visual Client ein neuer Benutzer angelegt wird. Dieser Umstand wurde jedoch nur bei der Standardinstallation mit Sicherheitsebene 0 aufgedeckt.

Fakt P-4: Aufzählung von System, Benutzer und Arbeitsbereich

Mit der P4-Befehlszeilenkonsole, dem P4V-Client sowie der P4Web-Benutzeroberfläche kann ein Angreifer neue Benutzer anlegen und dann die Perforce-Server, die Benutzer und Gruppen auf dem System, die verfügbaren Arbeitsbereiche und viele andere Leistungsmerkmale und Einstellungen des Servers durchsuchen. Mit folgenden Befehlen können sich Angreifer viele der Perforce-Einstellungen auflisten lassen, darunter auch das für den Benutzer beim Anmelden ausgegebene Ticket:

```
branches      Display list of branches
changes       Display list of pending and submitted changelists
changelists   Display list of pending and submitted changelists
clients       Display list of known clients
counter       Display, set, or delete a counter
counters      Display list of known counters
depots        Display list of depots
describe      Display a changelist description
diff          Display diff of client file with depot file
diff2         Display diff of two depot files
jobs          Display list of jobs
labels        Display list of labels
license       Update or display the license file
monitor       Display current running perforce process information
opened        Display list of files opened for pending changelist
protects      Display protections in place for a given user/path
sizes         Display size information for files in the depot
tickets       Display list of session tickets for this user
users         Display list of known users
workspaces    Display list of known clients
```

Durch die Möglichkeit solcher fast anonymer Aufzählungen bekommt ein Angreifer das Material für einen zielgerichteten Angriff praktisch frei Haus.

Fakt P-5: Alle Verbindungen zwischen Client und Server sind unverschlüsselt

Sämtliche Daten (einschließlich Quellcode), die zwischen P4Web-Client und Perforce-Server sowie P4V-Client und Perforce-Server ausgetauscht werden, können leicht ausgespäht und von böswilligen Benutzern im freigegebenen Netzwerk manipuliert werden. Das Fehlen der SSL-Verschlüsselung konterkariert gleich mehrere Aspekte der Anwendungssicherheit. In Frage kämen folgende Schwachstellen:

- Lauschangriffe
 - » Mit einem entsprechenden Sniffer können böswillige Benutzer von der Anwendung behandelte sensible Daten aufzeichnen.
 - » Mit einem Sniffer können böswillige Benutzer an Anmeldeinformationen gelangen, sich so selbst in die Anmeldung einloggen und für das Opfer ausgeben.
 - » Die Sitzungs-ID kann aufgezeichnet und bei der Herstellung einer Verbindung mit dem Server erneut abgespielt werden. Auch hier kann sich ein Angreifer als das vom Datendiebstahl betroffene Opfer ausgeben.
- Man-in-the-Middle-Angriffe
 - » Ohne SSL können sich Benutzer nie sicher sein, dass der Server auch tatsächlich das System ist, als das er sich ausgibt. Angriffe wie die Manipulation des Adress Resolution Protocol (ARP) oder des Domain Name System (DNS), böswillige Proxies und manipulierte „Host“-Dateien könnten dazu verwendet werden, den Datenverkehr des Opfers über das System des Angreifers zu leiten, ehe er beim Server ankommt.
- Datenbeschädigung
 - » Secure Sockets Layer (SSL) dient zur Authentifizierung der Remote-Webseite gegenüber dem Benutzer. Da genau dieser Datenverkehr nicht verschlüsselt ist, werden Teilnehmer nicht authentifiziert. Zudem gibt es keinerlei Integritätsprüfung der versandten Nachrichten. Einem Angreifer wäre es also möglich, Daten während der Übertragung zu verändern. Ohne SSL hat ein Angreifer praktisch die freie Auswahl, wie er die Daten beschädigen will.

Fakt P-6: Authentifizierte Benutzer bleiben angemeldet

Sobald sich ein Benutzer mit seinem Kennwort angemeldet hat, wird für ihn ein so genanntes „Ticket“ ausgestellt, das in der Regel 12 Stunden gültig ist und für dessen Dauer er dann auch angemeldet bleibt. Ein Angreifer kann dadurch also ohne Anmeldung auf das Perforce-Depot zugreifen und die Perforce-Benutzerdatenbank mittels Spoofing ausspähen.

Fakt P-7: Die Authentifizierung für P4Web lässt sich umgehen

Unsere Überprüfung hat gleich mehrfach Probleme mit der Authentifizierung ergeben. Zu den Sicherheitslücken mit dem höchsten Risiko zählt die Tatsache, dass die Tools nicht nach einer strengen Authentifizierung verlangen. Jeder beliebige Anwender kann eine Anforderung mit einem leicht zu erratenden Cookie-Wert nachstellen und sich so vermeintlich authentifizierten Zugang zum System erschleichen. Sobald das geschehen ist, kann er auf dem Perforce-Server sehr umfangreiche Befehle ausführen.

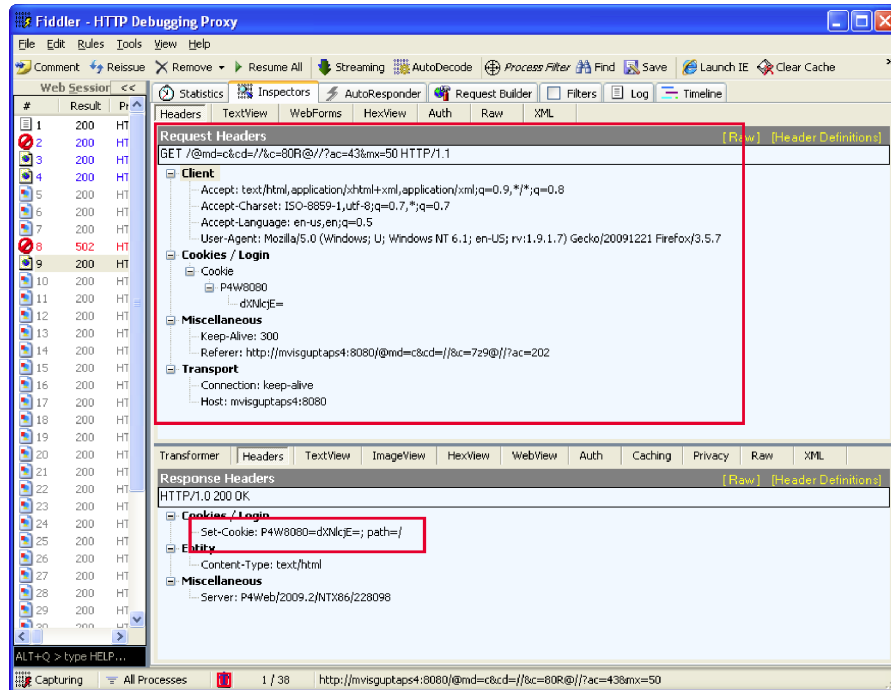


Abbildung 2: Das Sitzungs-Cookie ist die mit Base64 kodierte Fassung des Benutzernamens.

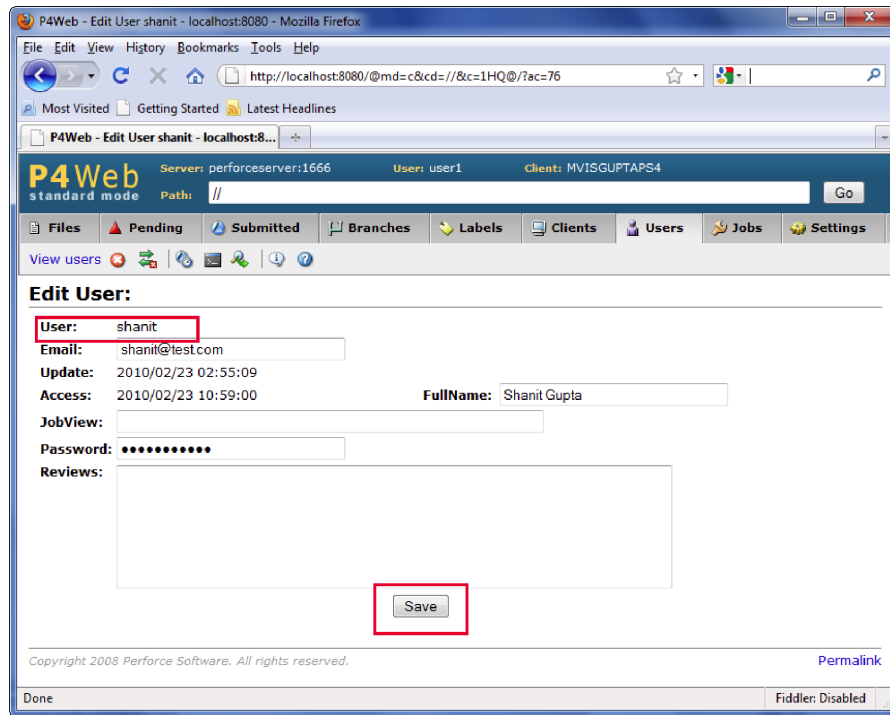
Um authentifizierten Zugang zu erhalten, muss der Angreifer eine Anforderung, wie im Screenshot oben, nachstellen. Wenn der Angreifer dabei die richtige URL angibt und ein Cookie mit dem Namen des Benutzerkontos des Opfers einrichtet, wird ihm authentifizierter Zugang gewährt. Der Name des potenziellen Opfers ist dabei leicht zu finden – er kann in der P4Web-Anwendung abgerufen werden.

Fakt P-8: Mehrere Fehler bei der Zugangsberechtigung

Während unserer Überprüfung sind uns mehrere Lücken in der Zugangskontrolle aufgefallen. So sind zwar bestimmte Konsolen, die angemeldeten Benutzern nicht zur Verfügung stehen sollten, in der P4Web-Internetschnittstelle unsichtbar. Durch Manipulation der URL und der übermittelten Parameter ist es jedoch möglich, andere Benutzer-, Client- oder Projektdaten zu manipulieren.

Die von dieser Sicherheitslücke ausgehende Gefahr potenziert sich noch, wenn zusätzlich die oben bereits genannten Fakten berücksichtigt werden. Denn mit einmal erlangter Zugangsberechtigung können Fehler bei eben jener Zugangsberechtigung ausgenutzt und ausgeweitet werden. Die Einflussmöglichkeiten etwaiger Angreifer steigen.

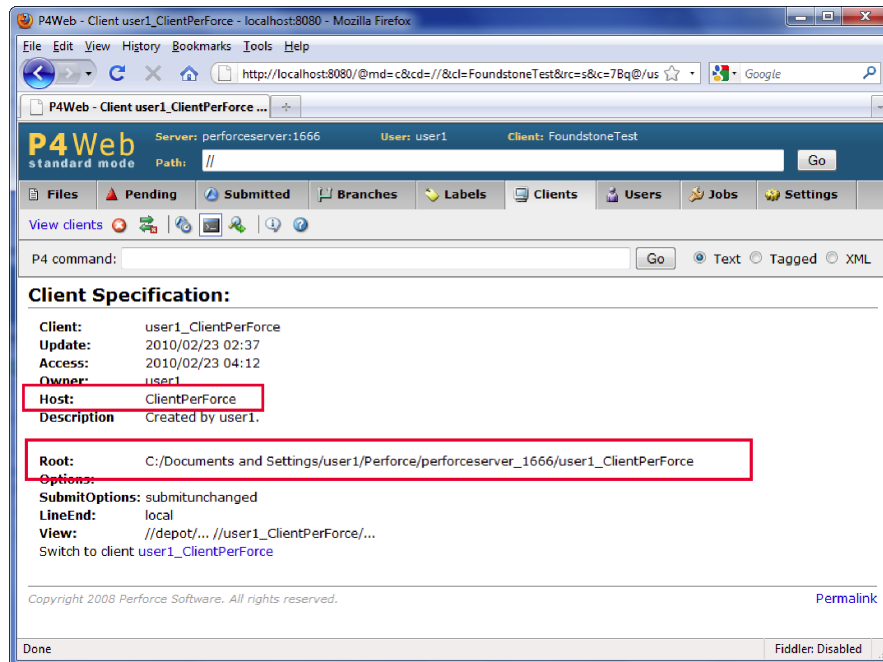
So sollte der angemeldete Benutzer in dem Screenshot auf der nächsten Seite („user1“) beispielsweise keinen Zugriff auf Benutzer „shanit“ haben. Durch Manipulation der URL und der übermittelten Parameter war es uns jedoch möglich, die Profilseite des Benutzers „shanit“ zu bearbeiten.



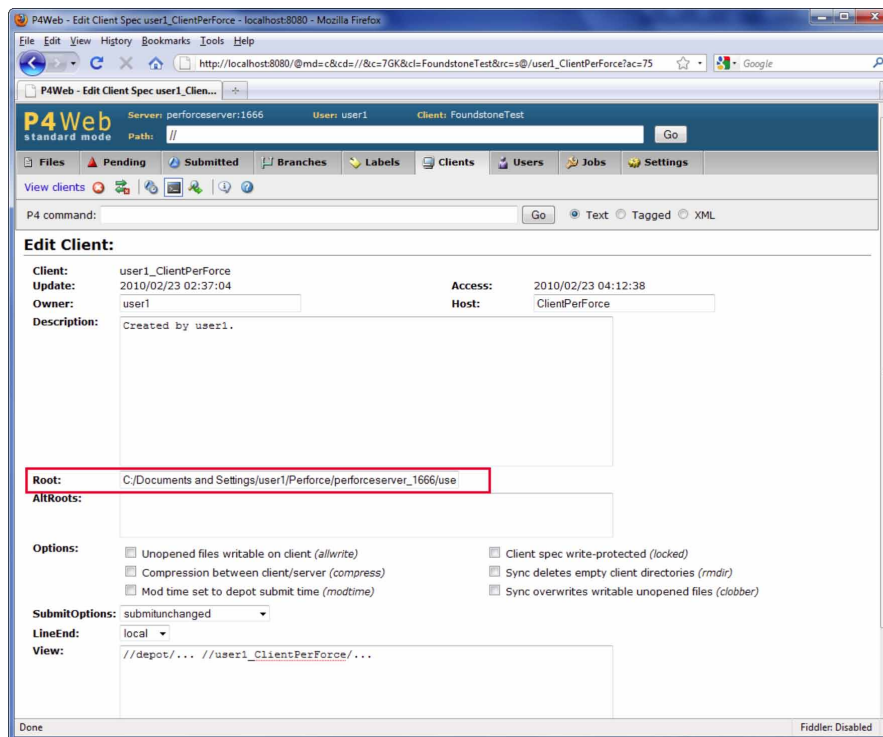
Fakt P-9: Verzeichnisdurchquerungen können zu Systemkompromittierung führen

Fehlerhafte Zugangsberechtigungen in Kombination mit unzureichender Zugangskontrolle für die Arbeitsbereiche von Benutzern ermöglichen potenziellen Angreifern eine so genannte Verzeichnisdurchquerung (Directory Traversal), durch die alle Dateien auf einem betroffenen System kompromittiert werden können. Schlimmstenfalls kann ein Benutzer in böser Absicht sogar sämtliche Dateien überschreiben oder die Daten der Windows-Sicherheitskontenverwaltung kompromittieren, um vollen Zugriff auf das betroffene System zu erlangen.

Alle Anwender der Perforce-SCM-Lösung haben einen Arbeitsbereich auf ihrem lokalen System. Dieser Arbeitsbereich ist ein lokaler Cache-Speicher der im SCM gespeicherten Dateien, wobei der Speicherplatz dieses Arbeitsbereichs vom Endbenutzer festgelegt wird. Böswillige Benutzer können dank der schwachen Zugangskontrolle das Verzeichnis des Arbeitsbereichs anderer Anwender ändern. So lässt sich das Stammverzeichnis des Arbeitsbereichs etwa auch in „C:\Windows“ oder jeden beliebigen anderen Verzeichnispfad ändern. Beim nächsten (manuellen oder automatischen) Dateiabgleich können die Dateien aus dem Arbeitsbereich so auf den Perforce-Server gelangen und anderen Anwendern zugänglich sein. Außerdem können Dateien – und somit auch wichtige ausführbare Dateien oder Konfigurationseinstellungen – im betroffenen Arbeitsbereich überschrieben werden. Das wiederum kann das ganze System in Mitleidenschaft ziehen.



Der angemeldete Benutzer sollte nur Lesezugriff auf den Client „user1_ClientPerForce“ haben. Deshalb gibt es für diesen Client auch keine Bearbeitungsschaltfläche „Edit“.

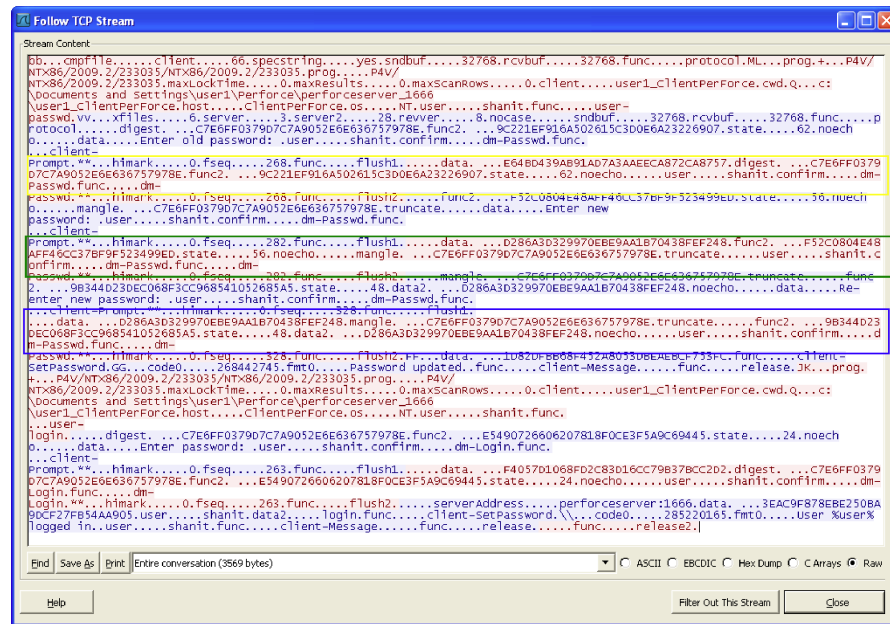


Durch Manipulation der URL und der Parameter kann der angemeldete Benutzer das Stammverzeichnis auf dem betroffenen System ändern und es an einen gefährdeteren Ort verlegen.

Fakt P-10: Unbefugte Kennwortänderungen sind möglich

Nach erfolgreicher Authentifizierung zwischen dem P4V-Client und dem Perforce-Server wird ein Sitzungs-Token ausgegeben, der zur Identifizierung einer Benutzersitzung verwendet werden kann. Es wird jedoch scheinbar nicht zur Änderung des Kennworts eingesetzt. Daher können böswillige Benutzer unbefugte Kennwortänderungen vornehmen.

Dazu muss der Angreifer eine Kennwortänderungssitzung einleiten und bei der ersten Anforderung seinen Benutzernamen und den Digest des aktuellen Kennworts senden. In der Anforderung mit dem Digest des neuen Kennworts und dem alten Benutzernamen kann er anschließend den Benutzernamen des Betroffenen und einen vom Angreifer gewählten Kennwort-Digest senden. Dieser Vorgang wird bei der Anforderung zur Bestätigung des Kennworts noch einmal wiederholt. Das Ergebnis: Der Angreifer hat das Kennwort seines Opfers geändert.



Der gelb hervorgehobene Abschnitt ist die mit Benutzernamen und Kennwort-Digest des angemeldeten Benutzers gesendete Anforderung. Der grün hervorgehobene Abschnitt ist die Anforderung mit dem neuen Kennwort-Digest. Diese Anforderung enthält auch den Benutzernamen. Ein böswilliger Benutzer kann nun aus diesem Benutzernamen den des Opfers machen. Analog dazu ist der blau hervorgehobene Abschnitt die Kennwortbestätigung. Auch hier kann ein böswilliger Benutzer aus diesem Benutzernamen den des Opfers machen und das Kennwort des Betroffenen ändern.

Fakt P-11: Journal- und Protokolldateien können von jedem ausgelesen werden

Standardmäßig installiert Perforce alle Dateien – also auch die Journal- und Protokolldateien des Programms – in allgemein lesbarer Form. Dadurch können Angreifer auch als Standardbenutzer sämtliche Einträge in den Journal- und Protokolldateien einsehen, einschließlich aller Datenbankaktualisierungen und Quellcode-Commits.

Fakt P-12: Perforce-Dateien als Klartext gespeichert

Der Perforce-P4V-Client und der Perforce-Server speichern alle Dateien als Klartext auf dem Client-Server-System.

Bei Kompromittierung des Entwicklersystems kann dies zu einer Kompromittierung des gesamten Codes im lokalen Speicher führen. Analog dazu macht die Klartextspeicherung aller Dateien auf dem Perforce-System auch den Code zu einem leichten Angriffsziel.

Fakt P-13: Konten haben standardmäßig weit reichende Rechte

Standardmäßig sind alle Benutzer auf dem Perforce-Server zunächst einmal Superuser mit den entsprechenden Berechtigungen. Das heißt, jeder Benutzer darf auf dem Perforce-Server Konten anlegen. Der erste Benutzer, der den Befehl „p4 protect“ ausführt, wird Superuser der Umgebung.



Zwar findet sich dieser Befehl so auch in der Dokumentation, einigen Administratoren ist jedoch nicht unbedingt bewusst, dass die Umgebung zunächst einmal abgesichert werden muss, ehe sie in einer nicht vertrauenswürdigen Umgebung geöffnet werden darf.

Fakt P-14: Socket Hijacking kann zu Kompromittierung von Informationen bzw. DoS-Angriffen führen

Ein nicht sicher eingebundener Socket kann von Angreifern gekapert werden, wodurch Angreifer die Kompromittierung von Informationen bzw. DoS-Angriffe einleiten können.

Dazu bindet der Angreifer den über das Netzwerk Daten empfangenden Socket an denselben TCP/UDP-Port (wie den angreifbaren Socket) und an eine spezifische IP-Adresse (eine der zugrunde liegenden IP-Adressen). Sendet der Client nun eine Verbindungsanforderung an den Server, kommt die Verbindung beim Daten empfangenden Socket des Angreifers (und nicht am eigentlichen Socket) an, da dieser eine bestimmte IP-Adresse überwacht. Der Client merkt nicht, dass er mit einem nicht autorisierten Socket verbunden ist, wodurch der Angreifer erfolgreich auf Informationen zugreifen kann. Weil zudem nie eine Verbindung zwischen Client und dem eigentlichen Socket zustande kommt, kann der Angreifer darüber hinaus erfolgreiche DoS-Angriffe gegen den Server starten.

Für die Ausnutzung dieser Sicherheitslücke benötigt der Angreifer nur minimalen Zugang zu dem System mit dem angreifbaren Socket: Er muss lediglich Code bzw. Anwendungen auf dem System ausführen können.

Gegenmaßnahmen

Folgende Empfehlungen können helfen, Server mit sensiblen Daten vor Angriffen zu schützen. Bei der Installation und Einrichtung eines sicheren SCM-Systems sollten dabei alle möglichen Angreifer und Angriffsmöglichkeiten in Betracht gezogen werden. Zu den potenziellen Angreifern gehören:

1. Insider (ohne böswillige Absicht) mit Zugriffsrechten
2. Insider (mit böswilliger Absicht) mit Zugriffsrechten
3. Außenstehende (ohne böswillige Absicht) mit Zugriffsrechten
4. Außenstehende (mit böswilliger Absicht) mit Zugriffsrechten

Hier nun unsere wichtigsten Erkenntnisse und Empfehlungen:

- *Vertraulichkeit und Integrität:* Bei Benutzerkonten wird das Sicherheitsprinzip „So wenig Rechte wie möglich“ allzu oft nicht beherzigt. Mit den Konten sind häufig unnötig viele Befugnisse für Funktionen innerhalb des Systems und hinsichtlich der eigentlichen Quellcode-Dateien selbst verbunden. Richtig und wichtig wäre es jedoch, die Berechtigung für administrative Funktionen ebenso einzuschränken wie den Lese- bzw. Schreibzugriff auf Quellcode und Quellcode-Strukturen. Denn sobald ein Angreifer einmal Administratorrechte erlangt hat, hat er auch das SCM-System voll unter Kontrolle, da es auf Administratorebene praktisch keine Einschränkung der Berechtigungen mehr gibt. Aus diesem Grund sollten Unternehmen zwar ihren Quellcode-Kontrollsystemen umfassenden Zugang gewähren – Benutzern hingegen nur die Rechte, die sie tatsächlich auch benötigen.
- *Protokolle, Audits und Unleugbarkeit:* Standardmäßig sind SCM-Systeme nur in geringem Maß für Protokollierungen konfiguriert. Stattdessen muss das System ausdrücklich so eingerichtet und konfiguriert werden, dass jeder Vorfall auf dem System protokolliert wird. Dazu gehören unter anderem Funktionstests des Quellcodes, Commits, Zweige und Änderungen der Konfiguration. Enthalten sein sollten zudem Benutzer, Datum und Uhrzeit sowie ausgeführte Funktion. Dies gilt insbesondere für wichtige Funktionen wie Versuche, die gesamte Struktur herunterzuladen und fehlgeschlagene Versuche, auf sensible Funktionen und Bereiche zuzugreifen. Zudem sollten Sicherungskopien von Protokolldateien erstellt und an anderen Standorten gespeichert werden, da nur so deren Integrität gewährleistet werden kann. Nach Möglichkeit sollte die Direktanmeldung auf einem anderen als dem SCM-System stattfinden. Unabdingbar ist letztlich auch die regelmäßige Überprüfung der Protokolldateien.
- *Verfügbarkeit:* Das SCM-System sollte gegen DoS-Angriffe sowohl vom Netzwerk und vom System als auch vom SCM-Programm selbst immun sein.
- *Authentifizierung:* Das System sollte eine zwei Faktoren basierende Authentifizierung (2FA) verlangen, um zu gewährleisten, dass es sich beim System anmeldende Benutzer auch um die handelt, die sie zu sein vorgeben. Das SCM sollte die auf zwei Faktoren basierende Authentifizierung möglichst erkennen und deren Charakteristika für die Zugangskontrolle nutzen. Einmal verwendbare Kennwörter können eine Alternative zur auf zwei Faktoren basierenden Authentifizierung darstellen. Zudem sollten sämtliche Benutzer- und Administratorkonten auf stillgelegte oder gelöschte Benutzer geprüft und diese gegebenenfalls entfernt werden.

- *Selbstschutz*: Das System muss in der Lage sein, seine Protokoll- und Konfigurationsdateien zu schützen und so Unterwanderungsversuche zu blockieren. Darüber hinaus müssen die für diesen Selbstschutz eingesetzten Algorithmen stark sein. Kryptologische Hash-Funktionen können eine gute Grundlage zur Bestimmung unbefugter Dateiveränderungen darstellen.
- *Sicherungskopien*: Es sollten regelmäßig Sicherungskopien erstellt werden, die den gesamten Quellcode erfassen. Die Integrität der Sicherungskopie sollte unabhängig validiert und alle Dateien mit einer digitalen Signatur versehen werden.
- *Verbindungen*: Das System verschlüsselt gespeicherte Daten ebenso wie gerade übertragene und verwendete Daten. Das bedeutet, dass sämtliche Verbindungen verschlüsselt sein müssen – egal ob es sich dabei um einen Datenverkehr durch einen sich beim System anmeldenden Benutzer, Zugriff auf einen bestimmten Zweig oder Ausführung anderer Aktionen handelt. Auch das Repository und alle Sicherungskopien müssen verschlüsselt werden.
- *Strategien für Patches und Konfigurationen*: Das Betriebssystem, auf dem sich die SCM-Software befindet, muss regelmäßig gepatcht sowie seine Konfiguration ständig überwacht und entsprechend den neuesten Bedrohungen aktualisiert werden. Dasselbe gilt für die Komponenten des SCM-Systems selbst.
- *Allgemeine Systemabsicherung*: Das SCM-System sollte nur einem einzigen Zweck dienen und keine anderen Funktionen als das Software-Konfigurations-Management haben. Das zugrunde liegende Betriebssystem sollte alle nicht zwingend erforderlichen Funktionen deaktivieren. Vor Einsatz des SCM sollten Administratoren einen guten und bewährten Rahmen für die Absicherung schaffen. Diesen bieten beispielsweise das US-amerikanische Gesetz zur Verwaltung von Informationssicherheit (Federal Information Security Management Act, FISMA) oder die Richtlinien der National Security Agency (NSA).
- *Netzwerkprotokollierung*: Wenn Hacker in ein System eindringen, können sie beliebige Änderungen an und auf dem kompromittierten System vornehmen. Es gibt nur wenige Möglichkeiten herauszufinden, wie genau der Angreifer Zugang zum System erlangte (um sich dann gegen künftige Angriffe entsprechend zu schützen). Eine dieser wenigen Möglichkeiten besteht im Nachvollziehen der Schritte des Angreifers mittels Netzwerkprotokollierung. Die meisten Unternehmen verfügen jedoch nur über Protokolldateien ihrer Netzwerkinfrastruktur, d. h. zu den Haupteintritts- und Austrittspunkten an der Firewall, zu VPN, E-Mail, Instant Messaging sowie zum Internet-, Netzwerk- und Router-Datenverkehr. Das reicht jedoch nicht aus. Darüber hinaus verfügen nur ganz wenige Unternehmen über forensische Netzwerksysteme, die sämtlichen Datenverkehr so speichern, dass ein Vorfall auch nach einem Ausfall analysiert werden kann. Dabei hilft gerade diese Gegenmaßnahme dabei, die Vorgänge während eines Angriffs wie Aurora wirklich zu erfassen.

Hinweis: Bedenken Sie, dass jeder dieser Fakten für alle Schnittstellen gilt, die von SCM-Systemen freigegeben werden. Unsere Erfahrung zeigt, dass es dabei häufig die selten verwendeten Schnittstellen wie Webschnittstelle und Eingabekonzole sind, auf die es Angreifer abgesehen haben. Diese dürfen also bei der Frage nach gründlicher Tiefensicherheit auf keinen Fall aus dem Blick geraten.

Empfehlungen speziell für Perforce

Neben den oben genannten allgemeinen Sicherheitsempfehlungen und -richtlinien möchten wir Ihnen nachfolgend auch einige Empfehlungen speziell zu Perforce geben. Sicherheitsempfehlungen von Perforce selbst gibt es zudem unter <http://kb.perforce.com/article/1173/basics-of-perforce-security> und unter http://www.perforce.com/perforce/conferences/us/2007/presentations/DSteele_Authentication2007.pdf.

Fakt P-0: Perforce führt eine allenfalls geringfügige Absicherung der Systeme durch, auf denen es installiert wird

Gegenmaßnahme: Sichern Sie das zu Grunde liegende System ab.

Unternehmen sollten entsprechend eine allgemeine Absicherung sämtlicher Systeme vornehmen, auf denen sich Quellcode befindet. Perforce-Server sollten dazu mindestens gemäß den Sicherheitsgrundregeln des Anbieters abgesichert werden. Zahlreiche Absicherungs-Benchmarks und Prüflisten finden Sie im Center for Internet Security (www.cisecurity.org) und beim National Institute of Standards and Technology (<http://web.nvd.nist.gov/view/ncp/repository>).

Fakt P-1: Der Perforce-Serverdienst (p4s.exe) und die Perforce-Webschnittstelle (p4webs.exe) werden mit Rechten auf SYSTEM-Ebene installiert

Gegenmaßnahme: Gewähren Sie dem Benutzer, unter dem p4s.exe und p4webs.exe ausgeführt werden, weniger Rechte.

Richten Sie auf Grundlage der Bedürfnisse Ihres Unternehmens einen Perforce-Benutzer mit so wenig Rechten wie möglich ein. Ändern Sie den aktiven Benutzer, indem Sie erst auf „Systemsteuerung“ -> „Verwaltung“ -> „Dienste“ klicken und dann mit der rechten Maustaste die „Eigenschaften“ des aktiven Perforce-Dienstes (Perforce und Perforce Web) auswählen und auf die Registerkarte „Anmelden“ klicken. Richten Sie für die Perforce-Anwendungen anschließend einen Benutzer mit so wenig Rechten wie möglich ein.

Fakt P-2: Nicht authentifiziertes Anlegen von Benutzern

Fakt P-4: Aufzählung von System, Benutzer und Arbeitsbereich

Fakt P-7: Die Authentifizierung für P4Web lässt sich umgehen

Fakt P-13: Konten haben standardmäßig weit reichende Rechte

Gegenmaßnahme für die Fakten P-2, P-4, P-7, P-13: Aktivieren Sie „Administrator“- oder „p4 protect“-Zugang.

Standardmäßig kann in Perforce jeder Zugriff auf vorhandenen Quellcode erlangen. Daher muss unter Perforce entweder ein Administratorkonto angelegt oder der Befehl „p4 protect“ ausgeführt werden. So bleibt der Zugang auf bestehende Benutzer beschränkt und der Zugriff auf den Quellcode kann kontrolliert werden. Von hier aus können Sie zudem Authentifizierung und Autorisierung von Benutzern auf sensible Daten im Depot beschränken. Achten Sie darauf, dass Sie dazu die höchste von drei Sicherheitsebenen aktivieren.

Fakt P-3: Viele Kennwörter sind nicht verschlüsselt

Gegenmaßnahme: Verwenden Sie Netzwerk- oder End-to-End-Verschlüsselung wie SSL für Layer 2 oder Layer 3.

Fakt P-5: Alle Verbindungen zwischen Client und Server sind unverschlüsselt

Gegenmaßnahme: Verschlüsseln Sie Datenverkehr mit SSL oder SSH.

Bei der Konfiguration von SSL-Sicherheit hat sich Folgendes bewährt:

- Einsatz eines einmaligen SSL-Zertifikats von einer vertrauenswürdigen Zertifizierungsstelle für jedes System (oder eines Platzhalter-Zertifikats, das denselben Zweck erfüllt)
- Deaktivierung der Unterstützung für das SSLv2-Protokoll, das wiederholt Ziel von Man-in-the-Middle-Angriffen und Downgrades der Verschlüsselung geworden ist
- Deaktivierung der Unterstützung für alle Verschlüsselungs-Suites mit Verschlüsselungen unter 128 Bits
- Deaktivierung der Unterstützung für alle Verschlüsselungs-Suites, die den Algorithmus „Anonymous Diffie-Hellman“ zum Schlüsselaustausch unterstützen
- Aktivierung von SSL für das Anmeldeformular sowie alle Seiten, die für den Zugang eine Authentifizierung verlangen

Mit dem Programm SSLDigger von McAfee Foundstone® können Sie testen, ob die SSL ordnungsgemäß konfiguriert wurde. SSLDigger kann unter <http://www.foundstone.com/us/resources/proddesc/sitedigger.htm> heruntergeladen werden.

Fakt P-6: Authentifizierte Benutzer bleiben angemeldet

Gegenmaßnahme: Legen Sie mithilfe der Option „TIMEOUT“ eine Zeitüberschreitung fest.

Fakt P-8: Mehrere Fehler bei der Zugangsberechtigung

Gegenmaßnahme: Sperren Sie den p4web-Zugang.

Fakt P-9: Verzeichnisdurchquerungen können zu Systemkompromittierung führen

Gegenmaßnahme: Sperren Sie den p4web-Zugang.

Fakt P-10: Unbefugte Kennwortänderungen sind möglich

Gegenmaßnahme: Dieses Problem wird in Version 2010.1 behoben.

Fakt P-11: Journal- und Protokolldateien können von jedem ausgelesen werden

Fakt P-12: Perforce-Dateien als Klartext gespeichert

Gegenmaßnahme für die Fakten P-11 und P-12: Schützen Sie das System vor Angriffen, bei denen Eindringlinge Benutzer- oder Administratorrechte für den direkten Zugriff auf das System erhalten.

Fakt P-14: Socket Hijacking kann zu Kompromittierung von Informationen bzw. DoS-Angriffen führen

Gegenmaßnahme: McAfee empfiehlt, die Sockets für den Datenempfang sicher zu machen, indem auf dem Socket selbst die Option für die Verwendung ausschließlich einer Adresse (SO_EXCLUSIVEADDRUSE) aktiviert wird. Dann kann der Socket nicht mehr gekapert werden. Mit diesem Prozess lässt sich zudem eine Zugriffssteuerungsliste auf dem Socket einrichten, wenn das System mit dem Betriebssystem Windows Server 2003 oder höher ausgeführt wird.

McAfee-Schutz

Für unsere Kunden gibt es eine Reihe von McAfee-Produkten, mit denen sich SCM- und Content-Management-Systeme besser vor Angriffen schützen lassen. Folgende McAfee-Technologien können helfen, Ihre Systeme künftig vor ähnlichen Angriffen zu schützen:

- *McAfee Vulnerability Manager:* Mittels Erkennung und Schwachstellenprüfung findet McAfee Vulnerability Manager SCM-Systeme in Ihrem Netzwerk ebenso wie Schwachstellen im System. McAfee Vulnerability Manager deckt so Sicherheitslücken in kompromittierten Systemen auf. Weitere Informationen hierzu erhalten Sie unter http://www.mcafee.com/de/enterprise/products/risk_and_compliance/.
- *McAfee Policy Auditor:* Mithilfe von Konfigurationsprüfungen bestimmt McAfee Policy Auditor die sicherste Konfiguration für ein System und spürt gleichzeitig Sicherheitslücken in kompromittierten Systemen auf. Weitere Informationen hierzu erhalten Sie unter www.mcafee.com/de/enterprise/products/risk_and_compliance.
- *McAfee Endpoint Encryption:* Der Einsatz von McAfee Endpoint Encryption verringert die Auswirkungen von Angriffen, indem der Zugang zu den Kernressourcen so eingeschränkt wird, dass Angreifer ihn erst aufwendig umgehen müssen. Weitere Informationen hierzu erhalten Sie unter www.mcafee.com/de/enterprise/products/system_security.
- *McAfee Data Loss Protection (DLP):* Der Einsatz der Lösungen McAfee Network DLP bzw. McAfee Host DLP ermöglicht es, das Extrahieren sensibler Daten wie Quellcode von außerhalb festzustellen und zu verhindern. Weitere Informationen hierzu erhalten Sie unter www.mcafee.com/de/enterprise/products/data_protection.
- *McAfee Configuration Control:* Mit dieser Lösung können Sie sämtliche Änderungen der Systemkonfiguration unterbinden, sodass Ihre SCM-Systeme nicht mehr so verändert werden können, dass sich sensible Daten aus ihnen extrahieren lassen. Weitere Informationen hierzu erhalten Sie unter www.mcafee.com/de/enterprise/products/risk_and_compliance.

Fazit

APTs erfreuen sich bei einer wachsenden Gruppe von böswilligen Angreifern zunehmender Beliebtheit. Ihre Ziele haben sich indes verschoben. Waren es früher Rechner der US-Militärindustrie, der Regierung und des Militärs, so sind es heute Konzerne, Unternehmen und der weltweite Handel. Dabei geht es in immer größerem Maße nicht mehr darum, die Rechner in den kompromittierten Unternehmen zu nutzen und auszunutzen, sondern darum, ganz bestimmte Daten und geistiges Eigentum zu stehlen. Es ist daher unabdingbar, dass Unternehmen proaktiv auf den Schutz ihrer wertvollsten Ressource – ihres geistigen Eigentums – hinarbeiten. Unternehmen müssen wissen, wo sich diese Ressourcen befinden, diese Systeme auf Sicherheitslücken und Fehlkonfigurationen überprüfen und vor Missbrauch und Angriffen schützen.

Mitwirkende und Danksagungen

Dieser Artikel ist das Gemeinschaftswerk zahlreicher McAfee Foundstone Professional Services-Berater sowie McAfee-Mitarbeiter, -Führungskräfte und -Forscher. Zu den wichtigsten Beitragenden gehören unter anderem Stuart McClure, Shanit Gupta, Carric Dooley, Vitaly Zaytsev, Xiao Bo Chen, Kris Kaspersky, Michael Spohn und Ryan Permech.

Bedanken möchten wir uns auch ganz herzlich beim Team von Perforce, das uns bei der Überprüfung der Fakten geholfen und mit uns Sofort- sowie Gegenmaßnahmen erarbeitet hat.

Über McAfee Labs

McAfee Labs stellt die Kerntechnologien und Bedrohungsanalysen bereit, die als Grundlage für die McAfee-Suite der Endgeräte-, Web- E-Mail- und Netzwerksicherheitsprodukte dienen. Unsere McAfee Labs-Forscher sind weltweit tätig und liefern genaue und zuverlässige Informationen zu weltweiten Bedrohungen. Die 350 multidisziplinären Forscher, die in 30 Ländern für McAfee Labs arbeiten, überwachen permanent das gesamte Bedrohungsspektrum, identifizieren Anwendungsschwachstellen, analysieren und korrelieren Risiken und arbeiten an Fehlerbehebungsmaßnahmen. Das McAfee Labs-Notfallreaktionsteam steht täglich rund um die Uhr zur Verfügung, um bestmöglichen Überblick über auftretende Risiken zu gewährleisten.

Über McAfee Foundstone Professional Services

McAfee Foundstone ist unangefochtener Marktführer auf dem Gebiet der Netzwerksicherheit. Hunderte bekannte Konzerne aus den Fortune 500 sowie Bundes- und Landesbehörden und das Militär nehmen unsere Beratungsdienste in Anspruch. Unsere externen Berater sind anerkannte Fachleute, Dozenten und technische Redakteure, die mit Ihrer Arbeit die gefährdetsten Organisationen der Welt schützen.

Über Perforce

Perforce Software entwickelt, vermarktet und unterstützt seit der Gründung 1995 das SCM-System Perforce mit dem Anspruch, das schnellste Software-Konfigurations-Managementsystem anzubieten. Perforce SCM versioniert und verwaltet Quellcode und digitale Ressourcen für kleine wie für große Unternehmen.

Perforce Software ist ein privatwirtschaftlich betriebenes Unternehmen mit Sitz im kalifornischen Alameda und weiteren Niederlassungen in Wokingham (Großbritannien) und Sydney (Australien).

Das Perforce SCM System wird heute von über 320.000 Entwicklern in 5.000 Unternehmen auf der ganzen Welt zur Verwaltung von Quellcode und digitalen Ressourcen verwendet.

