Burger Hut, Inc.
PCI Penetration Test

Security Assessment Report

Prepared for Burger Hut, Inc.
March 24, 2020 (version 1.0)

Table of Contents

Engagement Overview

Assessment Components and Objectives

Burger Hut, Inc. ("Burger Hut") recently engaged Atredis Partners ("Atredis") to perform a PCI Penetration Test of Burger Hut's retail environment and supporting backend infrastructure. Objectives included validation that Burger Hut's infrastructure and services were developed and deployed with security best practices in mind, and to obtain third party validation that any significant vulnerabilities present in Burger Hut's environment were identified for remediation.

Testing was performed from November 12 through November 29, 2020, by Jon Farmer and Maya Rodgers of the Atredis Partners team, with Damien Freeman providing project management and delivery oversight. For Atredis Partners' assessment methodology, please see Appendix II of this document, and for team biographies, please see Appendix III. Specific testing components and testing tasks are included below.

COMPONENT	ENGAGEMENT TASKS
Burger Hut PCI Penetration Test	
In-Store Systems and Network Infrastructure	• One sample in-store environment for penetration testing • Approximately 16 hosts with Linux, Windows and embedded platforms • 120 external in-store ISP connections for network discovery

HQ and SFO Network and Systems Infrastructure	• Internal network penetration testing
	  • Host and network enumeration and discovery
	  • Vulnerability enumeration and validation
	  • Controlled exploitation of identified vulnerabilities
	• Segmentation testing from internal non-CDE networks

Reporting and Analysis	
Analysis and Deliverables	• Status reporting and realtime communication • Comprehensive engagement deliverable • Engagement outbrief and remediation review

The ultimate goal of the assessment was to provide a clear picture of risks, vulnerabilities and exposures as they relate to accepted security best practices, such as those created by NIST, OWASP, or the Center for Internet Security. Augmenting these, Atredis Partners' also draws on its extensive experience in secure development and in testing high-criticality applications and advanced exploitation.

Engagement Tasks

Atredis Partners performed the following tasks, at a high level, for in-scope targets during the engagement.

Network and System Penetration Testing

Atredis performed traditional manual and automated network penetration testing against the in-scope targets, mapping out network services that were available, and confirmed the security-relevant aspects of these targets and services.

Once services were mapped out and confirmed, Atredis Partners used manual techniques along with automated network discovery and vulnerability discovery tools to assess the targets, built target-specific attack scenarios, and developed various engagement-specific tools to confirm the presence of vulnerabilities identified and reduce false positives, as needed.

Web Application Penetration Testing

For relevant external web applications and services, Atredis performed automated and manual web application penetration testing of web application components, applying generally accepted testing best practices as derived from the Open Web Application Security Project (OWASP) and the Web Application Security Consortium (WASC).

Testing was performed from the perspective of an anonymous intruder, identifying scenarios from the perspective of an opportunistic, Internet-based threat actor with no knowledge of the environment. Where relevant, Atredis Partners utilized both automated fuzzing and fault injection frameworks as well as purpose-built, task-specific testing tools tailored to the application and platforms under review.

Network Protocol Analysis

Atredis reviewed network traffic using various packet flow analysis and packet capture tools to observe in-scope network traffic with the objective of identifying scenarios where the integrity of trusted communications could be diminished or reduced. Network communications were analyzed for the presence of cleartext communications or scenarios where the integrity of cryptographic communications could be diminished, and Atredis Partners attempted to identify means to bypass or circumvent network authentication or replay communications, as well as other case-dependent means to abuse the environment to disrupt, intercept, or otherwise negatively affect in-scope targets and communications.

Executive Summary

Testing was performed with multiple user roles and access levels, specifically, Atredis was granted access to two instances of demo Burger Hut deployments, representing two sample customers, with admin and normal user level accounts, as well as API and file transfer access.

Atredis Partners performed testing initially from the perspective of an unauthenticated user, and mapped out the site structure, attack surface and session flow. Following enumeration activities, Atredis built test cases against each of the provided user roles, mapping out access levels for each account type and confirming that both lateral (user-to-user) movement and non-privileged user access to privileged functionality was disallowed.

In addition to web application security centric tasks, Atredis Partners also performed basic network vulnerability assessment of the environment, scanning for listening ports and fingerprinting network services to identify any network security relevant issues that might present a risk to the Burger Hut platform.

One element not tested in the testing environment was integration with a given client's authentication schema such as Active Directory (AD), doing so would have required access to a live customer environment.

Key Conclusions

Burger Hut places a high priority on network and system security, and while vulnerabilities were identified, many relate to a third party. In general, systems reviewed were consistently configured, patch management procedures were in place, and sensitive environments were properly isolated.

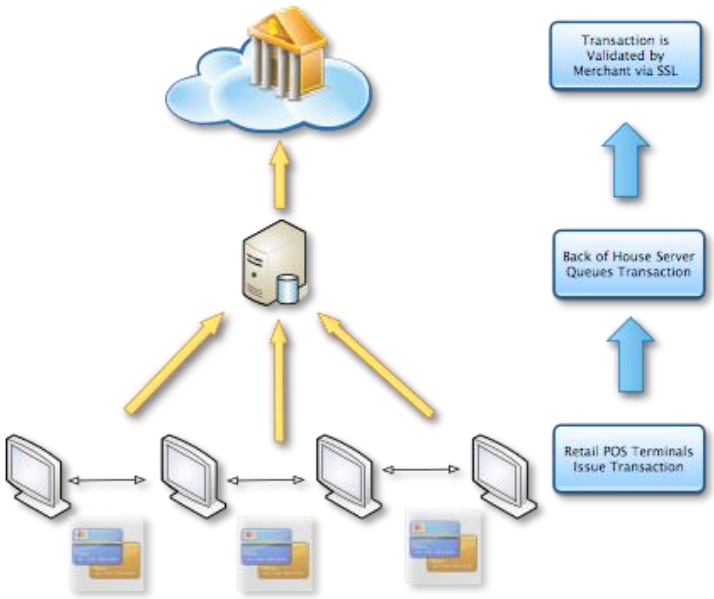
To further improve the defensibility of the environment, Burger Hut should review firewall management and intrusion detection capabilities with their third-party security provider, evaluate improvements in the credential management process, and continue to improve the patch and configuration management process to address any potential gaps.

PCI Environment Overview

Point of Sale (POS) Environment

Burger Hut makes use of the HPK CashPro POS platform, which is widely deployed by several large restaurant chains, in over 100,000 restaurants according to HPK. The platform runs on the Windows XP Embedded Operating System for touchscreen retail terminals. Magstripe readers and other peripherals such as cash drawers and receipt printers are attached, with terminals operating on the same network segment, allowing for shared transactions across stations and sharing of peripherals.

A `Restaurant Admin` server, running Windows 7 is dual-homed on both the POS network and an Internet-connected demilitarized zone (DMZ), and caches merchant transactions in the event Internet connectivity is lost. The `Restaurant Admin` server authenticates transactions against a few third-party merchant banks and serves as the desktop workstation for the restaurant manager. Restaurant Order Display Systems comprise of an LED screen and a lightweight embedded operating system, allowing kitchen staff to view and complete customer orders.



CashPro Platform Conceptual Dataflow

According to the CashPro documentation, CashPro 6.4 and above utilizes AES 256 for stored cardholder data and removes actual track data after a transaction is authorized, with some basic artifacts of the transaction such as authorization number stored for record keeping purposes. Based on Atredis' analysis of the Burger Hut lab and production retail environments, this statement appears to be accurate and involves a customized USB driver in use for the card reader and a proprietary key management scheme.

All instances of transactional records on the CashPro systems Atredis Partners were able to identify, either on terminals or `Restaurant Admin` systems, did not contain cleartext track data or card numbers. An in-depth reverse engineering of CashPro's encryption was not in-scope although Atredis observed the system appears to work as described by HPK. Authorization numbers and some other basic transactional information were present in the data.

The CashPro platform appears to rely on the magstripe reader's USB driver for cryptographic key management and it is Atredis Partner's conclusion that a memory-dumping rootkit with access to raw USB driver data could likely intercept cardholder data in cleartext. Still, this is typical in similar configurations outside of a trusted computing platform or a hardware-enabled cryptographic approach such as Chip and PIN.

Backend Environment and Network Security

Burger Hut contracts with Acme Security ("Acme") which manages a perimeter firewall in each store environment and provides managed Virtual Private Network (VPN) connectivity, log collection, and vulnerability scanning as well as a number of other PCI-centric security services.

Each store location initiates a VPN connection over a broadband connection to Burger Hut's Longview headquarters for centralized management and monitoring, with a cellular data backup connection as well as a backup management site located in a hosted facility in San Francisco. Backend and management services are typical, including centralized log collection, monitoring via Nagios, AD, and patch management. Acme's managed perimeter firewall ruleset is overall sound, with a default-deny policy. Only the `Restaurant Admin` server is permitted outbound connectivity, routing all corporate traffic down the VPN.

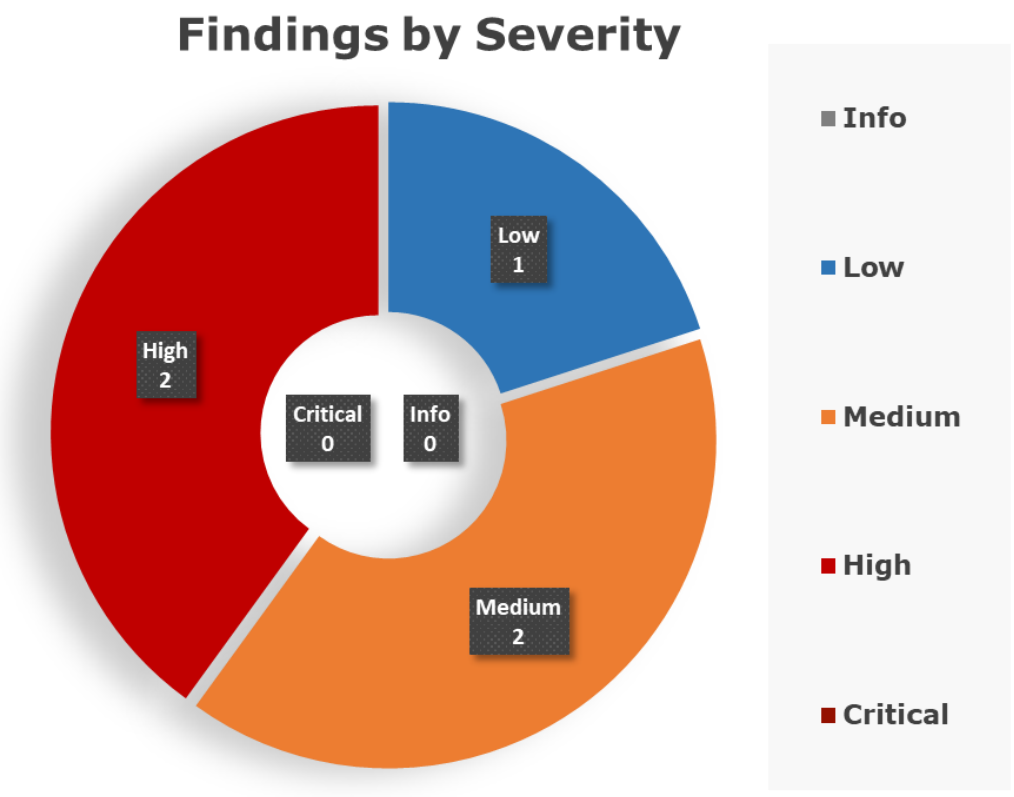
However, in the course of Atredis Partner's perimeter network discovery, Atredis noted one store location in New Jersey where the firewall had been disabled during the course of network troubleshooting, and this enabled Atredis Partners to compromise the firewall and gain access to the in-store environment as part of this engagement. We believe this underscores a need for Acme to perform a review of operational process as well as hardening of the MagicBox Linux firewall system and related applications.

Findings Summary

In performing testing for this assessment, Atredis Partners identified **two (2) high**, **two (2) medium**, **one (1) low** severity findings. No critical severity findings were noted. As stated earlier, none of these issues constitute a potential for direct compromise, and in the case of the medium severity vulnerability, other protections in the platform mitigate the issue.

Atredis defines vulnerability severity ranking as follows:

- **Critical:** These vulnerabilities expose systems and applications to immediate threat of compromise by a dedicated or opportunistic attacker.
- **High:** These vulnerabilities entail greater effort for attackers to exploit and may result in successful network compromise within a relatively short time.
- **Medium:** These vulnerabilities may not lead to network compromise but could be leveraged by attackers to attack other systems or applications components or be chained together with multiple medium findings to constitute a successful compromise.
- **Low:** These vulnerabilities are largely concerned with improper disclosure of information and should be resolved. They may provide attackers with important information that could lead to additional attack vectors or lower the level of effort necessary to exploit a system.



Remediation Tasks

In the case of this assessment, remediation tasks are not complex, and relate to configuration changes and general hardening practices. In remediating most findings, minimal (if any) changes to application source code are required, and no coordination with vendors or third parties is necessary to address findings.

As described elsewhere, no directly or indirectly exploitable conditions were noted from either an authenticated or unauthenticated user perspective, and as such, remediation tasks would be primarily driven by the objective of increasing overall application hardening and diminishing the impact of any potential future vulnerabilities that may arise in the platform.

Findings and Recommendations

The following section outlines findings identified via manual and automated testing over the course of this engagement. Where necessary, specific artifacts to validate or replicate issues are included, as well as Atredis Partners' views on finding severity and recommended remediation.

Findings Summary

The below tables summarize the number and severity of the unique issues identified throughout the engagement.

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	2	1	0

Findings Detail

FINDING NAME	SEVERITY
Misconfigured Perimeter Firewall	**High**
Weak Credentials and Authentication Bypass in MagicBox	**High**
IPMI Cipher Suite Zero Authentication Bypass	**Medium**
Multiple Vulnerabilities in Splunk Server	**Medium**
SSL Certificate Management Issues	**Low**

Misconfigured Perimeter Firewall

Severity: High

Finding Overview

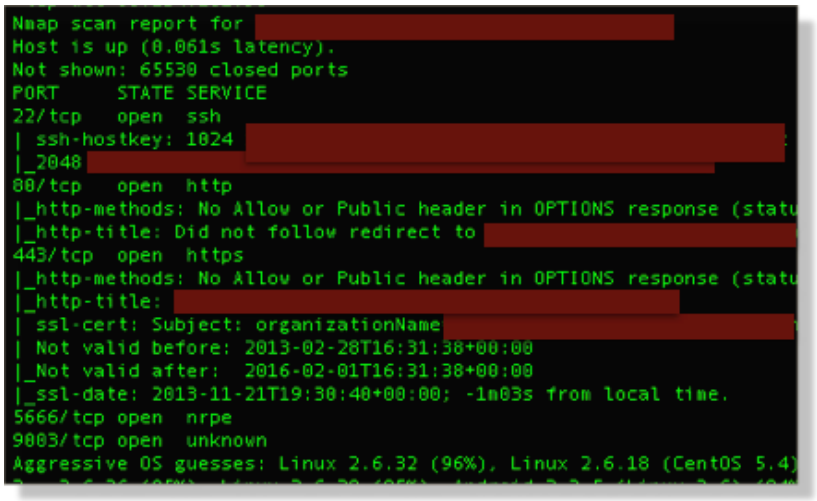
Insufficient network controls were found on the perimeter of a Burger Hut retail location which allowing access to network services which would otherwise be inaccessible to the general internet.

Finding Detail

In performing the network discovery of the external (internet-facing) interfaces of Burger Hut retail store locations, Atredis noted that one store (Store 39), had the firewall ruleset disabled. All other 126 stores provided store location IP addresses, offered no public services, and firewalls were correctly configured.

Upon further discussion with Burger Hut personnel, it was determined that network troubleshooting had recently taken place at this location, and that the firewall had been disabled during analysis and not subsequently re-enabled.

Atredis Partners then took steps to identify a means to gain shell access to the perimeter device, enumerating services and exposed applications. Atredis found two ways to compromise the device, after a few hours of analysis, based on previous review of the MagicBox device in the Longview lab. Specific vulnerabilities that allowed Atredis Partners to compromise this firewall are described in the next finding in this document.



Nmap Discovery Output for 1.1.2.2

Once Atredis obtained full `root` access, Atredis Partners re-applied the iptables ruleset located in `/etc/iptables/rules` to ensure the store environment was protected while also enabling persistent access for our testing team.

For approximately the following five days, due to the vulnerabilities discovered because of the disabled firewall ruleset, Atredis had full control of the `1.1.2.2` MagicBox device including access to all in-store devices and network traffic. With this level of access, interception of cardholder data and persistent command and control would be possible via a number of potential avenues, such as implantation of a memory-dumping rootkit in POS terminals, as described previously.

Atredis Partners performed minimal detection evasion steps and were not stealthy in compromise strategies. A number of Atredis attack patterns should have triggered host-level intrusion detection and log monitoring. At no time did Atredis Partners note any activity that would indicate the compromise was detected or that any alerts were triggered or responded to by monitoring personnel.

The Atredis team elected not to pursue more aggressive network infiltration into the retail network due to the potential for disrupting a live store environment.

Recommendation(s)

Burger Hut should task Acme Security with providing updated procedures around firewall ruleset management and detective controls such as local system log monitoring in the event a perimeter firewall is disabled. Host and network intrusion detection procedures should also be evaluated for their ability to detect unusual logon events.

References

NIST 800-41: Guidelines on Firewalls and Firewall Policy:
https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

Weak Credentials and Authentication Bypass in MagicBox

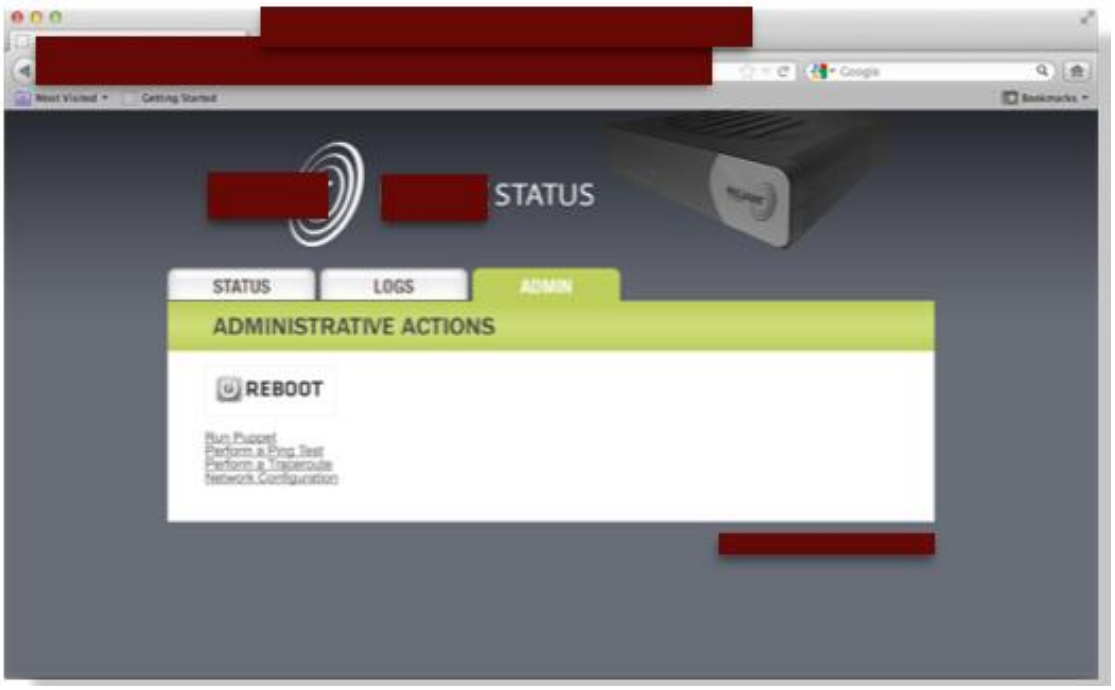
Severity: High

Finding Overview

Burger Hut's MagicBox devices were found to be utilizing a shared secret which allows attackers to bypass authentication and gain administrative access to the MagicBox system.

Finding Detail

In enumerating services on the misconfigured perimeter firewall device, Atredis Partners noted that the MagicBox administrative console offered a number of basic diagnostic utilities in its web interface via login. Despite a complex one-time-pad schema normally used for authentication, the admin service makes use of a stored secret value in session creation that is the same across all MagicBox deployments. Because Atredis was provided with an opportunity to review the MagicBox device in Burger Hut's Longview lab, Atredis Partners were able to determine this stored secret value and determined that these utilities interacted with a backend service that ran with `root` privileges.

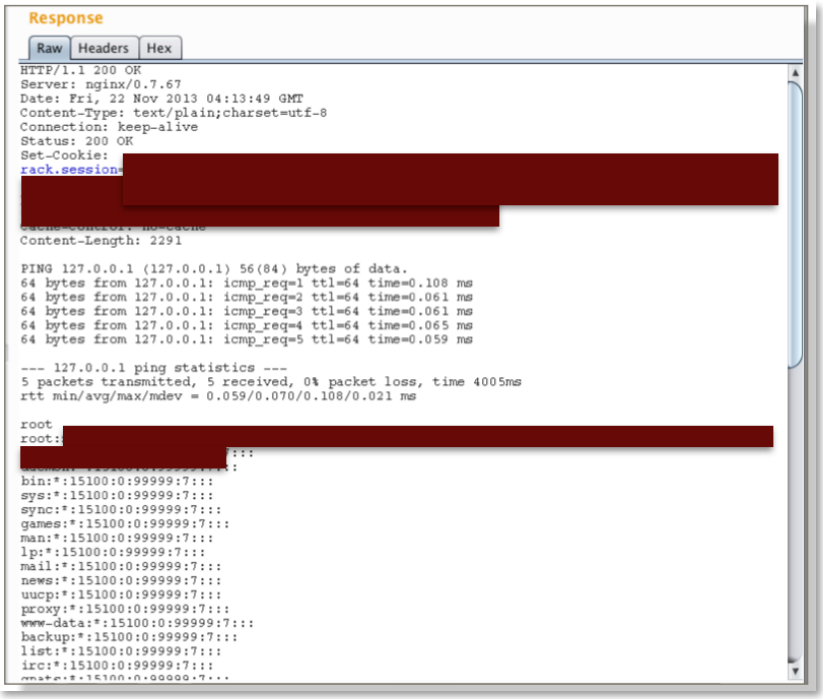


MagicBox Admin Console Web Interface

Once Atredis was able to bypass authentication by replaying this stored secret located in the `rack.session` HTTP header, Atredis Partners reviewed traffic to the `ping` (`/pingme URL`) utility in the admin interface. It was noted that the utility was vulnerable to a fairly trivial command injection bug.

Ping Test Command Injection Example

This service allowed Atredis to gain command injection as `root` and Atredis Partners were ultimately able to obtain usernames and passwords contained in the `/etc/shadow file`. After obtaining usernames and passwords, Atredis was then able to perform dictionary-based password cracking to gain a valid credential. Within a few seconds of loading the file into a password cracker, Atredis Partners noted the `install` user had a password of `install`. The `install` user did not have privileged (`sudoers`) access initially but was able to be added to an administrative group, thus obtaining full `root` access to the firewall via SSH.



Output of Ping Test Command Injection

Recommendation(s)

While the administrative services on the firewall device would normally be filtered to only authorized personnel, these interfaces and applications should still be defensible on their own as part of a defense-in-depth security model. This is especially critical for a perimeter device that provides security and monitoring services for other systems. Acme Security should seek out a third-party application source code review and web application penetration test, as well as perform a review of system and application hardening and software security development practices.

References

OWASP: Top Ten:
https://owasp.org/www-project-top-ten/

IPMI Cipher Suite Zero Authentication Bypass

Severity: Medium

Finding Overview

The Intelligent Platform Management Interface (IPMI) service, used on server console management platforms such as HP's iLO and Dell's DRAC, contains an authentication bypass when cipher suite zero (null encryption) is specified while connecting to a device. This allows an attacker with access to an affected server to power the server off, boot alternative media to load a rootkit, or perform any other attack that is possible with access to the server console.

Finding Detail

The following hosts were identified as allowing cipher suite zero authentication:

- `20.101.3.10`
- `20.101.3.11`
- `20.101.3.13`

Because affected devices are in a restricted disaster recovery DMZ with access only available via VPN to Burger Hut personnel who already have administrative access, Atredis Partners elected to rank this vulnerability as medium severity. If present on a general-use network such as a desktop Local Area Network (LAN), the finding would be ranked as high because it has potential to grant local administrative access. To confirm the vulnerability, use the free `ipmitool` utility.

Recommendation(s)

Vendor patches may be available to correct this issue, depending on the platform. If none are available, IPMI access should be restricted via network Access Control List (ACL).

References

Dan Farmer: IPMI Cipher Zero:
http://fish2.com/ipmi/cipherzero.html

CVE-2013-4783 Detail:
https://nvd.nist.gov/vuln/detail/CVE-2013-4783

Multiple Vulnerabilities in Splunk Server

Severity: Medium

Finding Overview

A number of undisclosed code execution and various web application vulnerabilities have been identified in the Splunk log collection and analysis server. Specifically, Splunk versions less than 4.3.6 are prone to cross-site scripting and clickjacking vulnerabilities, and versions less than 5.0.5 are vulnerable to remote code execution in certain contexts.

Finding Detail

Burger Hut's Splunk server (`20.100.3.20`) is managed by Acme and located in the Longview MagicBox Management DMZ. The server was identified as running Splunk 4.3.3, build `128297`, which was released in January, 2012, and this build has been unsupported since October, 2013.

Splunk Login Window with Build Number

Recommendation(s)

Update Splunk to the current, supported version, and identify gaps in the patch and configuration management process.

References

Bugtraq: 62632: Splunk Multiple Command Injection Vulnerabilities:
https://www.securityfocus.com/bid/62632

Bugtraq: 61537: Splunk X-Frame-Options Clickjacking Vulnerability:
https://www.securityfocus.com/bid/62632

CVE-2013-2766 Detail:
https://nvd.nist.gov/vuln/detail/CVE-2013-2766

SSL Certificate Management Issues

Severity: Low

Finding Overview

Numerous servers throughout the management environment were noted during testing as making use of self-signed Secure Sockets Layer (SSL) certificates.

Finding Detail

The following hosts were found to be utilizing self-signed SSL certificates:

- `20.101.0.30`
- `20.101.3.10`
- `20.101.3.11`
- `20.101.3.13`
- `20.101.10.30`
- `20.101.10.201`
- `20.101.10.202`
- `20.100.3.1`
- `20.100.3.20`
- `20.100.3.21`
- `20.100.2.1`
- `20.100.12.20`
- `20.100.12.30`
- `20.100.12.31`

In these instances, the hosts have no external validation and self-signed certificates allow an easy means for an attacker to impersonate a trusted service. Since the end user has already been trained in the security antipattern of clicking `accept` on an unauthenticated certificate, the user is likely to trust an attacker's impersonated certificate as well.

Burger Hut personnel noted that Acme Security's MagicBox systems make extensive use of self-signed certificates as well, and the MagicBox system Atredis gained access to made use of a self-signed SSL certificate. It is likely that all in-store MagicBox devices are affected as well.

In the case of Burger Hut internal systems, it is unknown to Atredis Partners whether an internal certificate authority is deployed on the internal AD domain. If so, systems listed in this finding managed by Burger Hut can be considered as unaffected.

Recommendation(s)

In this case, Burger Hut performs server-side session expiration so that sessions time out at reasonable intervals based on the number of active sessions. This mitigates the issue regardless of what value is supplied to the client side. Atredis recommends modifying the value sent to the client to a more reasonable value, as a stopgap in the event the server side timeout fails due to an error or an oversight.

References

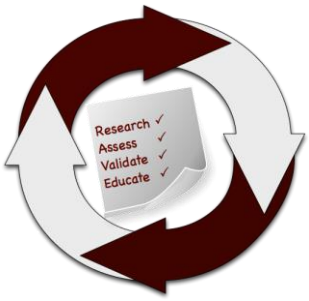
Microsoft: Active Directory Certificate Services Step-by-Step Guide: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772393(v=ws.10)?redirectedfrom=MSDN

Appendix I: Retail Store External IP Addresses

The following addresses are the 127 retail store ISP connection IP Addresses, as provided to Atredis by Burger Hut personnel on November 13, 2029. As described in this document, all but one of these addresses were configured with a default-deny firewall policy and no public services were identified.

123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X
123.456.789.X	123.456.789.X	123.456.789.X	123.456.789.X	

Appendix II: Assessment Methodology



Atredis Partners draws on our extensive experience in penetration testing, reverse engineering, hardware/software exploitation, and embedded systems design to tailor each assessment to the specific targets, attacker profile, and threat scenarios relevant to our client's business drivers and agreed upon rules of engagement.

Where applicable, we also draw on and reference specific industry best practices, regulations, and principles of sound systems and software design to help our clients improve their products while simultaneously making them more stable and secure.

Our team takes guidance from industry-wide standards and practices such as the National Institute of Standards and Technology's (NIST) Special Publications, the Open Web Application Security Project (OWASP), and the Center for Internet Security (CIS).

Throughout the engagement, we communicate findings as they are identified and validated, and schedule ongoing engagement meetings and touchpoints, keeping our process open and transparent and working closely with our clients to focus testing efforts where they provide the most value.

In most engagements, our primary focus is on creating purpose-built test suites and toolchains to evaluate the target, but we do utilize off-the-shelf tools where applicable as well, both for general patch audit and best practice validation as well as to ensure a comprehensive and consistent baseline is obtained.

Research and Profiling Phase

Our research-driven approach to testing begins with a detailed examination of the target, where we model the behavior of the application, network, and software components in their default state. We map out hosts and network services, patch levels, and application versions. We frequently use a number of private and public data sources to collect Open Source Intelligence about the target, and collaborate with client personnel to further inform our testing objectives.

For network and web application assessments, we perform network and host discovery as well as map out all available application interfaces and inputs. For hardware assessments, we study the design and implementation, down to a circuit-debugging level. In reviewing source code or compiled application code, we map out application flow and call trees and develop a solid working understand of how the application behaves, thus helping focus our validation and testing efforts on areas where vulnerabilities might have the highest impact to the application's security or integrity.

Analysis and Instrumentation Phase

Once we have developed a thorough understanding of the target, we use a number of specialized and custom-developed tools to perform vulnerability discovery as well as binary, protocol, and runtime analysis, frequently creating engagement-specific software tools which we share with our clients at the close of any engagement.

We identify and implement means to monitor and instrument the behavior of the target, utilizing debugging, decompilation and runtime analysis, as well as making use of memory and filesystem

forensics analysis to create a comprehensive attack modeling testbed. Where they exist, we also use common off-the-shelf, open-source and any extant vendor-proprietary tools to aid in testing and evaluation.

Validation and Attack Phase

Using our understanding of the target, our team creates a series of highly-specific attack and fault injection test cases and scenarios. Our selection of test cases and testing viewpoints are based on our understanding of which approaches are most relevant to the target and will gain results in the most efficient manner, and built in collaboration with our client during the engagement.

Once our test cases are validated and specific attacks are confirmed, we create proof-of-concept artifacts and pursue confirmed attacks to identify extent of potential damage, risk to the environment, and reliability of each attack scenario. We also gather all the necessary data to confirm vulnerabilities identified and work to identify and document specific root causes and all relevant instances in software, hardware, or firmware where a given issue exists.

Education and Evidentiary Phase

At the conclusion of active testing, our team gathers all raw data, relevant custom toolchains, and applicable testing artifacts, parses and normalizes these results, and presents an initial findings brief to our clients, so that remediation can begin while a more formal document is created. Additionally, our team shares confirmed high-risk findings throughout the engagement so that our clients may begin to address any critical issues as soon as they are identified.

After the outbrief and initial findings review, we develop a detailed research deliverable report that provides not only our findings and recommendations but also an open and transparent narrative about our testing process, observations and specific challenges in developing attacks against our targets, from the real world perspective of a skilled, motivated attacker.

Automation and Off-The-Shelf Tools

Where applicable or useful, our team does utilize licensed and open-source software to aid us throughout the evaluation process. These tools and their output are considered secondary to manual human analysis, but nonetheless provide a valuable secondary source of data, after careful validation and reduction of false positives.

For runtime analysis and debugging, we rely extensively on Hopper, IDA Pro and Hex-Rays, as well as platform-specific runtime debuggers, and develop fuzzing, memory analysis, and other testing tools primarily in Ruby and Python.

In source auditing, we typically work in Visual Studio, Xcode and Eclipse IDE, as well as other markup tools. For automated source code analysis we will typically use the most appropriate toolchain for the target, unless client preference dictates another tool.

Network discovery and exploitation make use of Nessus, Metasploit, and other open-source scanning tools, again deferring to client preference where applicable. Web application runtime analysis relies extensively on the Burp Suite, Fuzzer and Scanner, as well as purpose-built automation tools built in Go, Ruby and Python.

Engagement Deliverables

Atredis Partners deliverables include a detailed overview of testing steps and testing dates, as well as our understanding of the specific risk profile developed from performing the objectives of the given engagement.

In the engagement summary we focus on "big picture" recommendations and a high-level overview of shared attributes of vulnerabilities identified and organizational-level recommendations that might address these findings.

In the findings section of the document, we provide detailed information about vulnerabilities identified, provide relevant steps and proof-of-concept code to replicate these findings, and our recommended approach to remediate the issues, developing these recommendations collaboratively with our clients before finalization of the document.

Our team typically makes use of both DREAD and NIST CVE for risk scoring and naming, but as part of our charter as a client-driven and collaborative consultancy, we can vary our scoring model to a given client's preferred risk model, and in many cases will create our findings using the client's internal findings templates, if requested.

Sample deliverables can be provided upon request, but due to the highly specific and confidential nature of Atredis Partners' work, these deliverables will be heavily sanitized, and give only a very general sense of the document structure.

Appendix III: Engagement Team Biographies

Nathan Keltner, Founding Partner and CTO

Nathan Keltner leads, executes and coordinates advanced, custom-scoped projects for Atredis Partners. Nathan's primary focus includes hardware reverse engineering and penetration testing, red teaming, protocol analysis and private vulnerability research.

Experience

Nathan began his security career performing penetration tests and various security assessments for a large retail corporation, later expanding his career in consulting and specialization within red team penetration testing, exploit development, and software and hardware reverse engineering. Prior to starting Atredis Partners, Nathan most recently was a Senior Research Consultant on Accuvant's Applied Research team.

Nathan has also worked extensively as a penetration tester, helping design penetration testing methodologies and workflows as well as leading complex red team, social engineering, and attack simulation engagements, as well as numerous reverse engineering and binary analysis projects.

Nathan's research and exploitation assessments have recently focused on server hardware and embedded appliances, such as identification of vulnerabilities in BMC, UEFI, or OS firmware in related components. Previous expertise includes study of custom RF and ZigBee smart grid infrastructures, 802.15.4 and serial retail networks, multi-function ATM hardware and software, PIN entry devices, IPTV, VoIP hardware and software stacks, and modern networking access controls and identity management systems.

Key Accomplishments

Nathan has spoken at Black Hat USA, REcon, DEF CON, and other similar conferences on topics such as researching and exploiting smart grid radio frequency systems, exploitation in ARM TrustZone, advanced analysis of purpose-built system-on-chip architectures, and exploitation under limited-access user security models on the Windows platform.

Nathan holds a Bachelor of Business Administration degree in Management Information Systems from the University of Oklahoma, has held many information security and audit certifications over the years, and has been a frequent presenter at national and international security industry conferences.

Shawn Moyer, Founding Partner and CEO

Shawn Moyer scopes, plans, and coordinates security research and consulting projects for the Atredis Partners team, including reverse engineering, binary analysis, advanced penetration testing, and private vulnerability research. As CEO, Shawn works with the Atredis leadership team to build and grow the Atredis culture, making Atredis Partners a home for some of the best minds in information security, and ensuring Atredis continues to deliver research and consulting services that exceed our client's expectations.

Experience

Shawn brings over 25 years of experience in information security, with an extensive background in penetration testing, advanced security research including extensive work in mobile and Smart Grid security, as well as advanced threat modeling and embedded reverse engineering.

Shawn has served as a team lead and consultant in enterprise security for numerous large initiatives in the financial sector and the federal government, including IBM Internet Security Systems' X-Force, MasterCard, a large Federal agency, and Wells Fargo Securities, all focusing on emerging network and application attacks and defenses.

In 2010, Shawn created Accuvant Labs' Applied Research practice, delivering advanced research-driven consulting to numerous clients on mobile platforms, critical infrastructure, medical devices and countless other targets, growing the practice 1800% in its first year.

Prior to Accuvant, Shawn helped develop FishNet Security's penetration testing team as a principal security consultant, growing red team offerings and advanced penetration testing services, while being twice selected as a consulting MVP.

Key Accomplishments

Shawn has written on emerging threats and other topics for Information Security Magazine and ZDNet, and his research has been featured in the Washington Post, BusinessWeek, NPR and the New York Times. Shawn is a twelve-time speaker at the Black Hat Briefings and has been an invited speaker at other notable security conferences around the world.

Shawn is likely best known for delivering the first public research on social network security, pointing out much of the threat landscape still exists on social network platforms today. Shawn also co-authored an analysis of the state of the art in web browser exploit mitigation, creating the first in-depth comparison of browser security models along with Dr. Charlie Miller, Chris Valasek, Ryan Smith, Joshua Drake, and Paul Mehta.

Shawn studied Computer and Network Information Systems at Missouri University and the University of Louisiana at Lafayette, holds numerous information security certifications, and has been a frequent presenter at national and international security industry conferences.

Josh Thomas, Founding Partner and COO

Josh Thomas' specialties include advanced hardware and software reverse engineering, malware and rootkit development and discovery, and software development. Josh has extensive experience in developing secure solutions for mobile platforms and a deep understanding of cellular architecture. Josh previously held a TS clearance, and has worked in many sensitive, cleared environments.

Experience

Josh began his career 14 years ago in network administration and software development. Prior to moving his focus primarily to security, Josh wrote Artificial Intelligence and cryptographic solutions for the Department of Defense. Josh has extensive hands on knowledge of mobile devices and cellular infrastructure. He is also dedicated to hardware reverse engineering and embedded device exploitation.

Josh most recently was a Senior Research Scientist with Accuvant's Applied Research team and has worked as a Senior Research Developer at The MITRE Corporation. At MITRE, Josh performed analyses of the Android, Apple, Symbian and BlackBerry security models as well as other non-mobile embedded platforms and worked closely with the vendors and project sponsors.

Josh also developed an open-source mesh networking solution for Smart phone communications that bypasses the need for physical infrastructure, performed advanced spectrum analysis for cleared communications, and designed a secure satellite communications system required to handle the most sensitive communications possible while also being resilient against the highest levels of waveform interference.

Prior to his tenure at The MITRE Corporation, Josh developed Artificial Intelligence and embedded cryptographic solutions for General Dynamics and other organizations. Josh projects including the design and development of robust routing architecture for UAV/UGV autonomous vehicles, and battlefield troop movement predictive scenario generation.

Key Accomplishments

Josh is the recipient of three DARPA Cyber Fast Track grants for advanced security research, and has presented at multiple security industry conferences, including BlackHat, DEF CON, DerbyCon and ToorCon. Josh is the lead developer and maintainer of the open-source SPAN mesh networking project for Android, has published and reviewed papers for IEEE, and holds a pending patent related to NAND flash memory hiding techniques.

Josh holds a bachelor's in Computer Science from Texas A&M University and has been a frequent presenter at national and international security industry conferences.

Appendix IV: About Atredis Partners

Atredis Partners was created in 2013 by a team of security industry veterans who wanted to prioritize offering quality and client needs over the pressure to grow rapidly at the expense of delivery and execution. We wanted to build something better, for the long haul.

In five years, Atredis Partners has doubled in size annually, and has been twice named to the Saint Louis Business Journal's "Fifty Fastest Growing Companies" and "Ten Fastest Growing Tech Companies". In 2018, Atredis Partners joined the ranks of the Inc. 5,000 list of fastest growing private companies in the United States.

The Atredis team is made up of some of the greatest minds in Information Security research and penetration testing, and we've built our business on a reputation for delivering deeper, more advanced assessments than any other firm in our industry.

Atredis Partners team members have presented research over forty times at the BlackHat Briefings conference in Europe, Japan, and the United States, as well as many other notable security conferences, including RSA, ShmooCon, DerbyCon, BSides, and PacSec/CanSec. Most of our team hold one or more advanced degrees in Computer Science or engineering, as well as many other industry certifications and designations. Atredis team members have authored several books, including The Android Hacker's Handbook, the iOS Hacker's Handbook, Wicked Cool Shell Scripts, Gray Hat C#, and Black Hat Go.

While the Atredis client base is strictly confidential, and engagements often operate under stringent nondisclosure agreements, Atredis has delivered notable public security research on improving the security of Google, Motorola, Microsoft, Samsung and HTC products, and were the first security research firm to be named in Qualcomm's Product Security Hall of Fame. Atredis has received four research grants from the Defense Advanced Research Project Agency and has identified entirely new classes of vulnerabilities in hardware, software, and the infrastructure of the World Wide Web.

In 2015, we expanded our services portfolio to include a wide range of advanced risk and security program management consulting, expanding our services reach to extend from the technical trenches into the boardroom. The Atredis Risk team has extensive experience building mature security programs, performing risk and readiness assessments, and serving as trusted partners to our clients to ensure the right people are making informed decisions about risk and risk management.