uptech
Security Services

9021 Arboretum Parkway, Suite 140 • Richmond, VA 23236
info@uptechsecurity.com
(804) 213-2562

EXECUTIVE BRIEF

This report includes findings based on the vulnerability assessment against [redacted] in regards to the continuity, availability, and accessibility of [redacted]. Numerous high-level vulnerabilities were located, which deprecate the security and continuity of [redacted].

Based on the results of the phishing simulation, there is concern that specific end-users may inadvertently allow access to [redacted], and as such, allow the located vulnerabilities to be exploited which would result in a breach or business continuity issue. As such, nobody has to specifically "break in" to the network, one would merely use the inherent trust of end users and vulnerabilities in deprecated hardware and software to access or crash [redacted] or a segment thereof.

Though breach in itself does not have a criticality at first except potential loss of [redacted] efficiency, consider public trust if [redacted] had their information leaked. As we are all aware of, Equifax, Capital One, and other large corporations had a breach incident which deeply damaged their reputation. As a [redacted], the existence of a breach could be extremely detrimental to sales, resulting in not just a drop in customer trust, but also a potential [redacted].

While many machines show as highly secure, there are a large number that possess weaknesses that should be mitigated, many of which would require machine or device replacement. The machines that were found as secure were well maintained and ran more current versions of software and hardware. Traditionally, there is a three (3) year duty cycle on machines to ensure that hardware or software vulnerabilities that are not, or cannot be mitigated by the manufacturer are properly addressed.

In all, there were well over [redacted] critical level and exploitable weaknesses, many of which would result in a system crash. Many of these weaknesses were due to deprecation of machine age, or failure to balance machines in a configuration that would be a fault-tolerant environment and allow one machine to be taken offline for patch management and other necessary configurations. These vulnerabilities were, for the most part, [redacted] a lack of following the atypical three (3) year replacement strategy. It is the opinion of the investigator that proper and feasible funding, based on a five (5) year plan, be allocated to [redacted] to ensure viable security and continuity.

Additional concerns by the investigator again are the result of age, with many machines running a soon deprecated version of Microsoft Windows, and [redacted] in manufacturing running an [redacted]. While the Microsoft Windows issue can be mitigated by utilizing a new version of Windows, the investigator has concerns about the existing line of business applications properly running on a newer version of Windows. Nevertheless, support for a majority of the operating systems ends on January 14, 2020, so there is limited time to upgrade, though there is a high cost extended support option available from Microsoft. Additional funding should be earmarked for coding and development aspects to ensure all line of business applications are functional within newer versions of Windows.

Investigation should be made as to if the [redacted] manufacturer has updates available, though, based on findings, the investigator believes that replacement of [redacted] would be the most advantageous avenue based on total cost versus potential lost revenue. With the [redacted], the overall potential for continuity breach reducing production and availability of systems is extremely high. It is suggested by the investigator that inquiries be made into [redacted].

THIS SPACE INTENTIONALLY BLANK

EXECUTIVE SUMMARY

This overview presents the results of vulnerability assessment conducted on the [redacted] infrastructure. Results are limited to Wide Area Network, Internet Presence, Employee Security (Phishing), and Local Area Network interconnected devices including routing, switching, computers, printers, and telephony. Additionally, social engineering was utilized to make determination of information that may not otherwise be available within standard attack deltas.

The investigator makes no guarantee, express or implied that every single vulnerability has been located, and as such reported on, or that there are not false-positive results within the report. Due diligence was conducted to validate each device and exploit unless said exploit could potentially cause a loss of continuity to the respective device.

The overall methodology of the assessment was in a manner that fell under the category of cooperative/hostile. The cooperation was from the primary investigator in which information on critical vulnerabilities was released to [redacted] of the investigation conclusion to expedite the mitigation of weaknesses. Due to the mission critical nature of [redacted], when vulnerabilities that had the potential to crash or otherwise affect the tested system, the respective exploits were not run to protect the continuity and availability of [redacted].

[redacted] was following best practices in monitoring and reporting, and with the exception of not contacting law enforcement followed standard operating procedures. Initial footprinting of the network was detected by the [redacted] and immediately reported to management. The response time and monitoring of [redacted] infrastructure was handled in a prompt and professional manner, however, [redacted] configured in a sub-par manner, one [redacted] of which the default credentials were used [redacted] allowing the investigator to locate additional devices.

Additionally, [redacted] were found to have default administrative passwords, which, at minimum allowed the modification of network settings [redacted] IP conflict with other devices. It is the opinion of the investigator that [redacted] is considered as a second priority [redacted], which shows deep weakness within the [redacted] infrastructure. Efforts should be made to ensure that all [redacted] devices within the network are secured with, at minimum, an 8-character password for the [redacted]. Secure passwords would make more sense; however, almost any password would secure against pedestrian attack. For the sake of brevity, only those [redacted] with excessive issues are listed, however, all [redacted] within the multiple subnets of the [redacted] were, at the time of examination, running with either no password to administration, or factory default passwords.

However, in discussions, while the management of internal computing systems is managed by [redacted], routing, switching, and printing are managed by a third party. The investigator feels that utilization of said third parties has caused numerous weaknesses that would otherwise not exist and recommends a post-hoc test once the located issues outlined within this document are mitigated.

Sections within the technical reporting under the heading of [redacted] were validated only if the proof of findings had no risk to the continuity, integrity, or availability of the machine. In that case, other tests were conducted to validate expected responses or strings, and testing which could not be conducted due to aforementioned issues erred on the side of caution and were listed as vulnerabilities to ensure potential, yet unsubstantiated weaknesses were also addressed in a timely manner.

WIDE AREA NETWORK FINDINGS

Investigation was conducted on the Wide Area Network (WAN), or technically the outside facing network, which has the Classless Inter-Domain Routing (CIDR) of [redacted], and it was noted that best practices were, in no way, followed. As an initial introduction, a virtual private network (VPN) gives outside users' access [redacted]. For this to be effective and secure, the VPN should be difficult to find by a layman or attacker, and be well protected from one who finds the VPN connector. Nonetheless, while best practice dictates that to reduce the risk of scanning there not be a [redacted] and that the range utilized by VPN be in center range. There will be no further reporting as to the Wide Area Network, as security controls are in place, though best practices are not being followed. Adding information to the final report, in itself, will show no weakness to the overall infrastructure configuration other than the investigator concern relating to where the VPN is located.

Center range is best described as "if you have a number from one to ten, you pick five". The reason for going mid-line is that the majority of attackers look for the "low hanging fruit," in that they scan the top 25 and last 25 for an attack due to the time. If it takes too long to find any exploitable targets, the attacker moves on. Additionally, the use of a [redacted], while making it easier for users, gives out too much information in that it explains in the naming that the VPN in use is [redacted], as such provides attackers with more information than normally expected or accepted. [redacted]

To test network monitoring, the investigator first started with a stealth attack to footprint the network layout, and at the end of investigation conducted very overt, often reckless attacks against the [redacted] with no prevention procedures or blocking of the attacking IP addresses. Proper monitoring should have quickly noted anomalies and either flagged a system administrator or immediately blocked the offending addresses. For overt purposes the investigator instituted a [redacted] attack in which multiple tools attack a specific IP address or range within seconds of each other over a prolonged timeframe. This went undetected or, if detected, unreported, though conversations with the investigator and the primary [redacted] noted it was mentioned that the network team monitoring the virtual private network noticed some "minor issues."

It was outside the scope of work to specifically crash any system. No other findings other than the aforementioned VPN and real-time monitoring concerns arose during the external network testing.

[redacted]

LOCAL AREA NETWORK FINDINGS

The scan of the internal network was performed to validate the level of damage or potential data leakage which could happen assuming an attacker either breached external defenses or was able to infect an internal machine with remote access tools, normally through the means of malicious software [redacted]

Due to the fault-tolerance of some systems within [redacted], the reporting may include redundancies of issues based on findings. Finding are listed on a per-IP basis, and each vulnerability with a score of 4.0 and above is listed.

An overview of the located machines and devices within [redacted] network showed that there were multiple high-level or critical vulnerabilities which, mostly related to poor patch management and/or poor configuration. It should be noted that upon discovery of critical vulnerabilities, [redacted] was immediately notified so that mitigation strategies could be accomplished. The mitigation [redacted] Albeit, it should be noted that seven days after [redacted] was notified of a critical vulnerability in a [redacted] that mitigation **had not** been performed. Multiple [redacted] were located with default credentials in place, inclusive of [redacted]. A large quantity of the located [redacted] listed in the [redacted], providing a limited amount of continued support. In the opinion of the investigator, [redacted] makes the most sense for the company, even with the higher total cost of ownership (TCO). A centralized management of all organizational devices within one location, with failover to another would enhance security and allow deeper insight into usage.

It should further be noted that best practices are not being followed within the network, as there are deprecated versions of multiple Operating Systems that lose all support [redacted]. For example, Windows Server 2008 r2 is utilized heavily and reaches end of support on January 14, 2020. Many other machines are running Windows 7 Enterprise which also reach end of support on the same date. However, there is concern by the investigator that all applications would properly work on current versions of Operating Systems, as based on the last release of Windows 10 and Server 2019, many legacy class applications were blocked from running due to "security" concerns by Microsoft. Until it is validated that all necessary line of business applications properly run on Windows 10, investigation should be made into the Windows 7 and Windows Server 2008r2 extended support option from Microsoft which will be available for three (3) years after the January 14, 2020 deadline, albeit with a high cost and a per-device licensing model.

Additionally, the investigator has concern relating to network management and the findings that overly lackadaisical Virtual Local Area Networks (VLAN), specifically inter-VLAN routing (IVLR) is in place where two-way routing would not specifically be needed. Inter-VLAN routing allows specific subnetworks to "talk" back and forth to each other.

It is the opinion of the investigator that unless inter-VLAN routing is needed between segments that there should be no specific ability to traverse between subnetworks. For the sake of argument, if the network management LAN needs to access any subnet in particular the management LAN should have full access in a one-way manner. The investigator should not have access to every vLAN from a single subnetwork unless network design and configuration was poorly instituted at the network inception.

Under best practices, there should be a segmentation of network, frequently by Virtual Local Area Network (VLAN) segmentation. The current routing equipment in use is able to ensure segmentation of networks, including guest networks and is manageable by a local or cloud-based encrypted dashboard.

The overall assessment, which this report is written from, overviews, and outlines discernable issues that can be mitigated, with mitigation strategies provided to assist administrative and information technology staff. Specific vulnerabilities are critical in nature and should be addressed post-haste, as some vulnerabilities are overly simple to exploit and a single malicious attacker or employee could exploit the weaknesses to either access elevated permissions or crash [redacted].

Many devices within the local area network utilize S[redacted]. This is an immediate failure of any test as [redacted] not only releases specific information about the device, but also allows for denial of service or obtaining information which would otherwise be hidden from view. [redacted] should either disable [redacted] if not being used, or upgrade to [redacted], [redacted], and secure them with strong passwords. Take note that historically the [redacted] *can* allow changing of passwords by rewriting the [redacted] and allowing attackers to take control of routing and switching equipment.

Interim fixes for servers, be they Windows, Linux, or VMWare would best be addressed by cloning existing servers to a second one, clustering the machines, and taking one machine offline for patching, then performing the same action on the second.

INTERNET PRESENCE FINDINGS

There were no major finding noted on the Internet presence at [redacted] exception of the investigator ability to conduct cross-site scripting XSS, and the fact that the designed left a signature within the source code, to wit, [redacted] No developer name should ever be in source code. Were the investigator looking for a website, even for study purposes, they would attempt to hire the developer, request a similar site, and then use the full code to exploit the existing website as most developers reuse code on multiple Web sites.

There were additional minor findings of importance, especially with third party scripts being utilized within the Internet presence, which give a mixed-mode content on secure socket layers, in other words, the security of the site is at risk due to the developer not including secure links to scripts. Specific scripts include those obtained from [redacted]. Efforts should be made to ensure these specific pages and associated scripts are utilizing https.

There will be no further reporting as to the Internet Presence, as there are no specific security issues other than the aforementioned concerns by the investigator. The purpose of the final report is to outline vulnerabilities, and other than the investigator concern in relations to minor coding issues, there were no discernable vulnerabilities.

WIRELESS NETWORK FINDINGS

There were no major findings noted on the Wireless network with the exception of the guest network which not only showed an SSL error on connection, but also allowed access to the guest gateway. Testing of other wireless networks was conducted from outside the perimeter of the [redacted] by use of a General Dynamics GD8200 with a 30dBi Yagi directional antenna. Though networks were found, based on the criticality of devices within the [redacted], deauthorization attacks were not utilized. In lieu of deauthorization attacks, the investigator ran multiple password attack tools based on a sixteen-gigabyte dictionary file with no success. Assuming no deauthorization attack to obtain the encrypted password hash, and then time to attempt to crack said hash, the private wireless network is considered as inherently secured.

The guest wireless network shows the gateway of [redacted] which provides more information about the network than should be rendered by a guest network. There should be rules in place to mask addresses, segment traffic, and prevent "talking back" to any device that is on the same, or different networks. Basic consumer-class [redacted] can prevent traversal, and in the opinion of the investigator there is no reason that prosumer and corporate class devices cannot have a gateway on the same subnetwork and implement firewall rules to prevent any visible connectivity to any other network segments.

Lastly, one wireless network shows as being Wireless Equivalent Protocol (WEP) which is not near best practices. The network with WEP appears to list as [redacted]. WEP has multiple weaknesses, and just about everyone over the age of 13 years old knows about them. While WEP is better than having no password, it is not much better. There are multiple automated tools, that even on the slowest device can crack WEPP within minutes (Appendix G).

TARGETED PHISHING FINDINGS

Initial phishing testing was performed based on addresses that could be located by the investigator using various social networking platforms and internal located resources. Unfortunately, that list was minuscule in nature, though one user did click through within the first 20 minutes of test 1. To achieve a more accurate overview of phishing and how it would affect the organization as a whole, a full list of addresses was provided to the investigator which provided some very disturbing results. Of [redacted] failed with either clicking on links, entering personal information in forms, or otherwise not following best practices. While a unique breakdown by user shows a reasonable percentage of direct failure, the final breakdown of the test shows that out of [redacted] completed the respective training. Full charts and graphs are available within the section labeled as "phishing" within this document. A list of users will not be included in this document, however, upon request of [redacted] will be provided on an as-needed basis. The goal of the phishing engagement is not to ostracize or reprimand users, merely show a weakness in either training or attention by employees.

It is suggested that all employees receive phishing training, either by video or virtual conference. The level of users that failed the test, especially after attending training [redacted] is extremely concerning. Even with exploit mitigation in place, many "zero day" attacks will bypass SPAM filtering. The investigator made themselves part of the phishing engagement, left [redacted] filtering in place at "high" level, and 12 of the 15 attacks came through to the inbox.

No further reporting will be conducted as to phishing other than the graphs and charts of attack vectors and number of respective users. Replicating the same information within the reporting, which showing a vulnerability would merely be doubling the same information portrayed in this section.

DEVICE MITIGATION OVERVIEW

Each device is listed individually within the following report, and the report includes hot-linked access to the machines or devices within the PDF version of the report. Under each individual subnetwork, the affected devices are listed by address, with the first section being an overview with assumptions, and the second section describing the respective "fix" for the affected machine. There are very few vulnerabilities that are unable to be fixed, and those specific vulnerabilities are due to vendor lack of update, deprecation of hardware, or firmware.

Recommendations can be located at the end of this document under the heading of [redacted]

This concludes the executive summary aspect of the report.