Aman Toor

September 18, 2023

Professor:

CSCY-1050

**Ethyon Corporation Assessment Report**

**INTRODUCTION**

WizardSpyder consultant group engaged in the assessment and penetration test of the Ethyon Corporations Project Phoenix’s architectural system. The following report will evaluate the security of the Ethyon Corporation system by a risk rating conducted by WizardSpyder. Using the vulnerabilities discovered in the assessment and including the questions previously conducted beforehand by the WizardSpyder consultant group, the risk rating will be assigned.

On the Behalf of the WizardSpyder group, Ethyon Corporation, and the Canadian & USA government I have been granted permission to conduct an assessment of the Ethyon corporations project phoenix infrastructure. The Vulnerabilities that have been brought to light have been discovered through the use of Tools with respected Techniques and methods that highlight the security risk factors of the discovered vulnerabilities.

**1.2 Provided statements/information.**

Prior to the in-depth progression of the Ethyon Corporations infrastructure assessment, a Questionnaire was conducted to support the grey box methodology in which the WizardSpyder will be using to assess the system. The Grey box testing by WizardSpyder corporation involves around the partial knowledge of the internal system at work within the selected organization. This partial knowledge is provided within the Rapid assessment excel document with items listed all the way from LTE.1.0 – LTE.16.6.

Items LTE.1.0 to LTE.16.6 are categorized by their initial integer representing their categorized subject, followed by the question number you are viewing by their respected category. Listed below are the Item categorized number and their respected category name.

|  |  |
| --- | --- |
| **ITEM #** | **Category Name** |
| LTE.1.0 | Risk Management |
| LTE.2.0 | Security Policy |
| LTE.3.0 | Organizational Security |
| LTE.4.0 | Human Resource Security |
| LTE.5.0 | Asset Management |
| LTE.6.0 | Access Control |
| LTE.7.0 | Cryptography |
| LTE.8.0 | Physical Security |

|  |  |
| --- | --- |
| **ITEM #** | **Category Name** |
| LTE.9.0 | Operations Security |
| LTE.10.0 | Communications Security |
| LTE.11.0 | System development |
| LTE.12.0 | Supplier Relationships |
| LTE.13.0 | Incident Management |
| LTE.14.0 | Business Continuity |
| LTE.15.0 | Compliance |
| LTE.16.0 | Privacy |

Prior to the Assessment Ethyon has also provided the security standards coaligned with each question with their respective responses within the Rapid Assessment excel Document. These Security Standards can be revised and reviewed by their ISO reference Number as well as the ISO reference section title.

To assure that a thorough testing assessment is conducted of Project Phoenix’s system is done, Ethyon corporation has provided the Systems IP address to begin the process. The IP address is used to establish a thorough scan of the architectural systems for available ports that can be used tested and checked for any possible vulnerabilities. These ports can be opened for exploitation to infiltrate the systems inner workings, Hence the IP address (192.168.1.127) will be used to conduct many of the assessment checks and used with the pairing of selected tools for testing.

**1.3 Risk Rating**

WizardSpyder Consulting group has assigned a method of rating risks after an Assessment has been conducted and finalized. A risk rating is evaluated by a vulnerability’s severity meaning the harm it can bring to an organization, against its likelihood of occurring. The following risk rating indicates the possible levels of a vulnerability, and the way in which a vulnerability can be designated to a risk rating.

* **Critical**
  + Critical vulnerabilities in ETHYON are those which attackers with access to the organization’s internal network could leverage to obtain full compromise of affected hosts. Attackers could conduct post compromise activities on the affected hosts to expand and escalate their permissions across ETHYON’S active directory structure.
* **High** 
  + High-criticality vulnerabilities in ETHYON’S internal systems include those which sophisticated attackers could leverage to obtain full compromise of those systems under specific circumstances.
* **Medium** 
  + Medium-criticality vulnerabilities described in this report include those which could be used by an attacker in their execution of man-in-the-middle or client-side attacks against ETHYON’S systems and employees.
* **Low**
  + Low-criticality vulnerabilities are vulnerabilities that represent limited risk, but these vulnerabilities could be used in conjunction with other higher severity vulnerabilities, or social engineering, to compromise ETHYON’S systems.

A risk rating also identified as an Overall Risk rating can be essentially determined through a chart publicly available, the rating ultimately still relies on the information connected to the vulnerability’s severity against likelihood of happening.

**image 1.1**

A blue squares with orange squares

Description automatically generated

**Likelihood/Probability**

Determining the probability of a vulnerability being exploited is determined by the assigned tester. Probability is calculated by many factors that go towards it.

* factors include:
  + the time it takes to exploit the vulnerabilities the first time.
  + the time it takes to recreate the exploit once discovered.
  + Is there information from scanning or via http website that can point towards the vulnerability’s discovery (service name and version).
  + What information regarding these vulnerabilities can be discovered online in forums or upload pages such as GitHub.

Essentially these Factors are determined by the ability to locate the information for exploitation via reconnaissance stage. As well as the process of executing the vulnerabilities exploitation methods and other forms of factors that may show case them self in the process.

**Severity/Impact**

Determining severity relies on the outcome of the tested vulnerability and exploitation method. A ETHYON corporations Vulnerability that is assign a risk rating of critical must hold outcomes of, or similar, in the aspect in which the bad actor is given escalated privilege such as root over a inner working system.

**Detailed process and Findings**

The Following section of the assessment report aims to provide detailed clarifications. These clarifications will include the WizardSpyder consultant groups detailed steps taken to fulfill the agreed upon assessment of the Ethyon corporations Project Phoenix system. These steps consist of the broken of stages of Reconnaissance, Scanning, and Analysis.

**2.1 Reconnaissance**

The stage in which the Tester collects information regarding the target system, network, and organization. During the Assessment process of project Phoenix’s System, WizardSpyder Reconnaissance process involved the utilization of the assessment questionnaire (recall section 1.2). following forwards with the understanding of the assessment questionnaire document. The Document highlighted multiple alarming discovery regarding information in Ethyons system security and business management security.

The Excel document highlighted concerning responses; these responses consisted with a large value of the response “NO” within the document for certain listed Items questions. The majority of concerning responses arise from Items LTE 1.0 to LTE 9.14. Indicated below are responses for questions that WizardSpyder discovered concerning and possible leads for vulnerabilities and exploitation.

|  |  |  |
| --- | --- | --- |
| LTE.1.2 | Are risk assessments performed periodically to address changes in security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, when significant changes occur, etc.? | No |
| LTE.3.0 | Is there a dedicated information security team/function? **Genius: Please provide a copy of an organizational chart (specific to the information security team).** | No |
| LTE.5.8 | Is media disposed of in a secure manner using formal procedures when no longer required? Genius: Please provide a copy of the disposal and re-use of media policy. | No |
| LTE.6.0 | Is there an approved access control policy? Genius: Please provide a copy of the access control policy. | No |
| LTE.6.1 | Is access provisioned based on the principle of least privilege? | No |
| LTE.6.2 | Is there an approved remote access policy? Genius: Please provide a copy of the remote access policy. | No |
| LTE.6.5 | Is the allocation and use of privileged access rights restricted and controlled? | No |
| LTE.9.9 | Are event logs (e.g. user activity, exceptions, faults, etc.) being generated, retained, and regularly reviewed? Genius: Please provide sample log reviews. | No |

Each individual questions and responses alert a concerning issue regarding to security vulnerabilities in the project Phoenix system. Diving deeper into the questions different inferences can be discovered.

|  |  |
| --- | --- |
| LTE.1.2. | With risk assessments not being addressed periodically this can lead to large and vast amounts of vulnerabilities being unidentified. These unidentified vulnerabilities can then lay dormant till a bad actor discovers them; this’ll lead to an increase in security risk possibility. |
| LTE.3.0. | The lack of dedicated team in charge of security functions such as reviewing logs, checking for system updates and other aspects regarding keeping security at check is alarming. This can lead to attackers being free to exploits vulnerabilities in Project phoenix’s servers without being viewed and watched by dedicated Security teams. |
| LTE.5.8. | Improper or in ability to dispose of sensitive media, such as documents, hard drives, or other storage devices, ethically and properly can lead to data breaches and unauthorized access. Project phoenix’s lack of attention to this procedure can lead to financial implications, and work progress being halted. Attackers can obtain data by physical means such as discovering hard drives or storage devices from onsite garbage where storge holding data can be thrown if not discarded properly. |
| LTE.6.0. | Without an approved access control policy users can use an employee credential to remote access to servers and temper with data and information without the need for escalating privileges. Using this information for the security assessment we can assume that any Ethyon corporation credential can obtain access to project phoenix data and systems. |
| LTE.6.1. | similar LTE.6.0. the lack of access control policy such as a principle of least privilege can allow for compromised credentials to access project phoenix servers. With least privilege principle it can allow for Ethyon employees not associated with Project phoenix from access their system and information. Due to the missing principle the risk possibility of this possible vulnerability increases. |
| LTE.6.2. | Recalling back to LTE.6.0. The absence of a remote access policy can further increase the risk possibility within the Project phoenix, as bad actors are free to use any remote access capability Ethyon has incorporated in the system. |
| LTE.6.5. | Without access rights being restricted or control this puts the organization in jeopardy. A bad actor can create a personal credential and provide itself privilege in the project phoenix system and access and modify any data it choses to do so. |

Concluding the Reconnaissance stage of the assessment, we at WizardSpyder discovered multiple issues in Ethyon corporations Project Phoenix system. Many concerns in our discovery aim towards the policy engagement questions and as well as lack of dedicated security team. These issues lead to possible assumption of vulnerabilities where we can obtain access simply through a Ethyon employee whose account has been compromised.

**2.2 Scanning**

The stage in which a tester scans a target system looking for open ports, services, and potential risks on these port/services. During this stage WizardSpyder aim is to utilize a vast variety of tools. These tools consist of commands and applications such as, Nmap, Burpsuit, searchsploit, and other well known scanning tools.

During the Scanning process we at WizardSpyder conducted a Nmap scan to provide information of any open ports available on the System IP address 192.168.1.127. Utilizing a specific command that scans for any ports from a range of ports 1 to 65535 being used and also are classified as “open”. An Open port implies that Project Phoenix servers are utilizing those specific ports. The command utilized is as indicated “Nmap -p1-6535 192.168.1.127 --open”. Recalling Internal and External VA findings pdf Image 1 showcases the internal findings of the Nmap scan, presenting all possible ports with their service names associated with the port numbers.

During the scanning process, vulnerabilities that were discovered and associated with the open ports that we discovered were attached in the internal and external findings pdf. These vulnerabilities have been classified as Critical risk rating. The following table showcases the port numbers, service names, and Vulnerability.

|  |  |  |
| --- | --- | --- |
| Ports | Service | Critical vulnerability |
| 135 | MSRPC | * MS17-010 EternalBlue Vulnerabilities * Dropbear SSH Server < 2016.72 Multiple Vulnerabilities |
| 139 | netbios-dns | * DNS Server Dynamic Update Record Injection |
| 445 | Microsoft-ds | * Unsupported Windows OS (remote) * Microsoft SQL Server Unsupported Version Detection (remote check) |
| 3389 | ms-wbt-server | * Dell iDRAC Buffer Overflow Vulnerability |

Following these discoveries of vulnerabilities, I utilized a second scan methods. This scan methods aims to search its database for any exploitation methods that can be used against this vulnerability. Something that can be noted is that risk rating can also be considered by the factor of how many methods of exploitation are possible to be utilized against this vulnerability. The command executed for this assessment is as follows “Searchsploit” followed by the vulnerability name/title.

A screen shot of a computer

Description automatically generated

Through a Thorough scan using Searchsploit, certain information was brought to our attention. A scan of ms17-010 Eternalblue showed that project phoenix is vulnerable to smb remote code injections. This can be further confirmed with the vulnerability to Dropbear SSH Server, this vulnerability is exploitable by a ssh exploits if the operating system is on a windows 2016 system. And as noticed in the vulnerability to Microsoft-ds we find that project is running an unsupported OS suggesting that the systems operating system in use in a window 7 or 8.1 using a 2016 system update. Hence project phoenix is both vulnerable to exploit methods of a SMB remote code and SSH exploits. The SMB exploit can also be confirmed by a ms17-010 Nmap validation as located in image 2 of the internal and external findings VA pdf.

**2.3 Analysis**

After a Thorough Reconnaissance and Scanning stage we at WizardSpyder consultant group have discovered multiple related issues regarding the Ethyon Corporations Project phoenix System. These discoveries consisted of concerning issues of the structure in which the Phoenix is operating on from policy issues to risk management structure. Operating structure aside we have also assessed the system structure and the risks the vulnerabilities discovered have been based on a risk rating provided by WizardSpyder.

Attached in the Internal and external finding VA PDF is a list indicates all findings in regard to vulnerabilities discovered. These vulnerabilities have been assessed and provided risk rating escalating from low risk level to a critical risk rating. As reviewed previously this report has covered the critical risk rating vulnerabilities and their exploit possibilities. As stated in WizardSpyder consultant groups work layout we are adhered to provide a response such as mitigation methods and solutions for critical issues and concerns we discover.

After analysing the collection of info and concerns, we at WizardSpyder have chosen select methods that can be of support in mitigating and correcting any vulnerabilities in Ethyon corporations Project phoenix system. To begin with It has come to our attention that a rework of the corporation’s Organizational policy needs to be conducted or a revisory of the organizations policy. There are many concerns in the policy, one example of such is there is no implementation of a dedicated information security team. The lack of an information security team allows for the risk of bad actors tempering with directories without the worries of an individual watching logs for suspicious activity. Implementing a dedicated security team will allow for constant watch of logs and allow for quick reaction time for response to suspicious activity.

Another concern that was discovered was the vulnerabilities the phoenix project system is vulnerable to. Suggestions to mitigate the risks of these concerns includes creating a task force team involved in updating and repairing any outdated machines and systems that have been notified as threats to the organizations operation. Other mitigation methods are also reviewing authorized users’ policy and implementing a principle of least privilege to prevent Ethyon employee not involved in project Phoenix to access sensitive information not authorized to them. Adding access controls such as this and other principles will also allow for decrease in risk of bad actors using remote connect to access the system.

**Summary**

In conclusion on the behalf of WizardSpyder corporation this concludes the assessment report of the Ethyon Corporations Project phoenix System. Through the assessment many details have been looked over and discovered and thoroughly logged in this report. Many of these concerns and vulnerabilities have been brought to attention and given a risk rating, included has been suggestion going forwards with mitigating these risks. Furthermore a detailed listing of all possible vulnerabilities that have not been disclosed in this report are provided in a separate document titled “Internal and External VA findings “pdf containing all findings and commands executed.