ITMS 543 – Vulnerability Analysis and Control

Recon a website

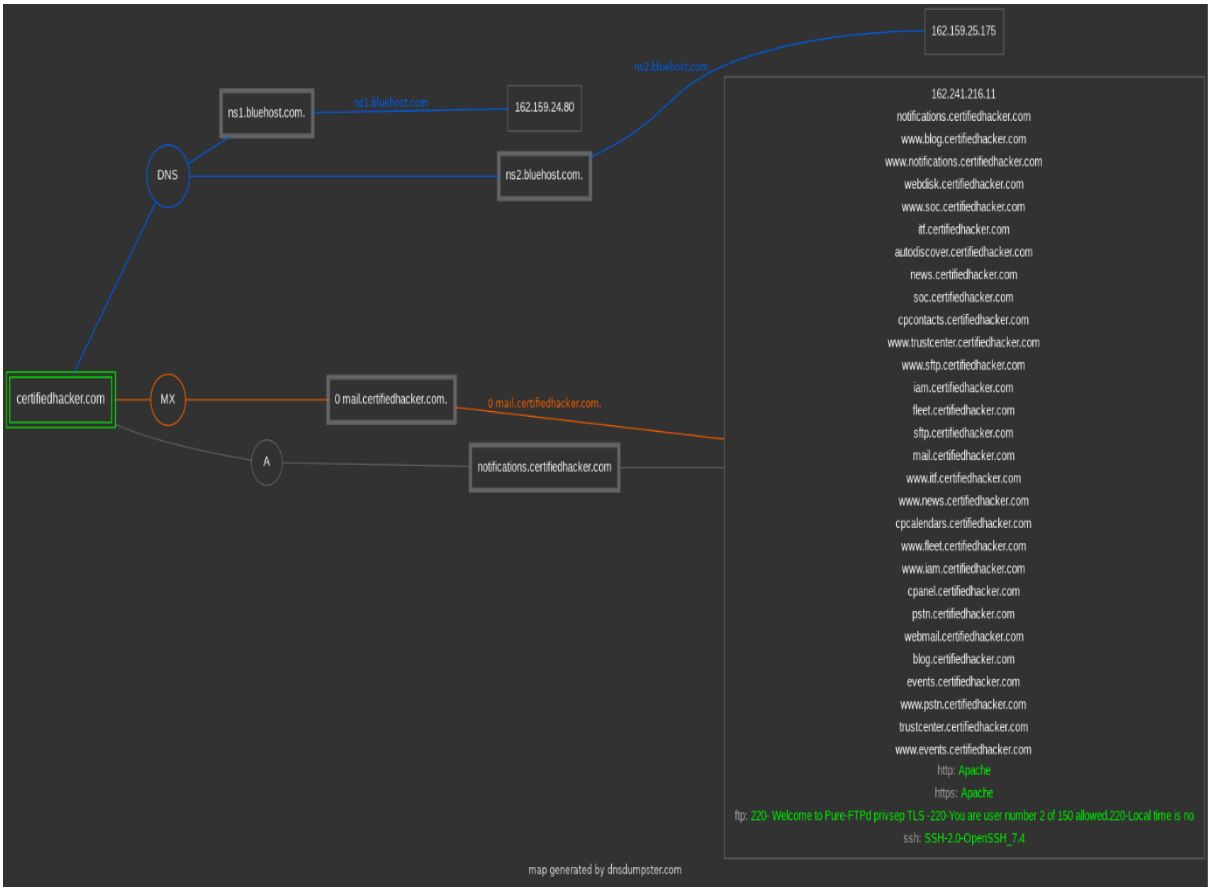
Rajabinandhan Periyagoundanoor Gopal

Executive summary

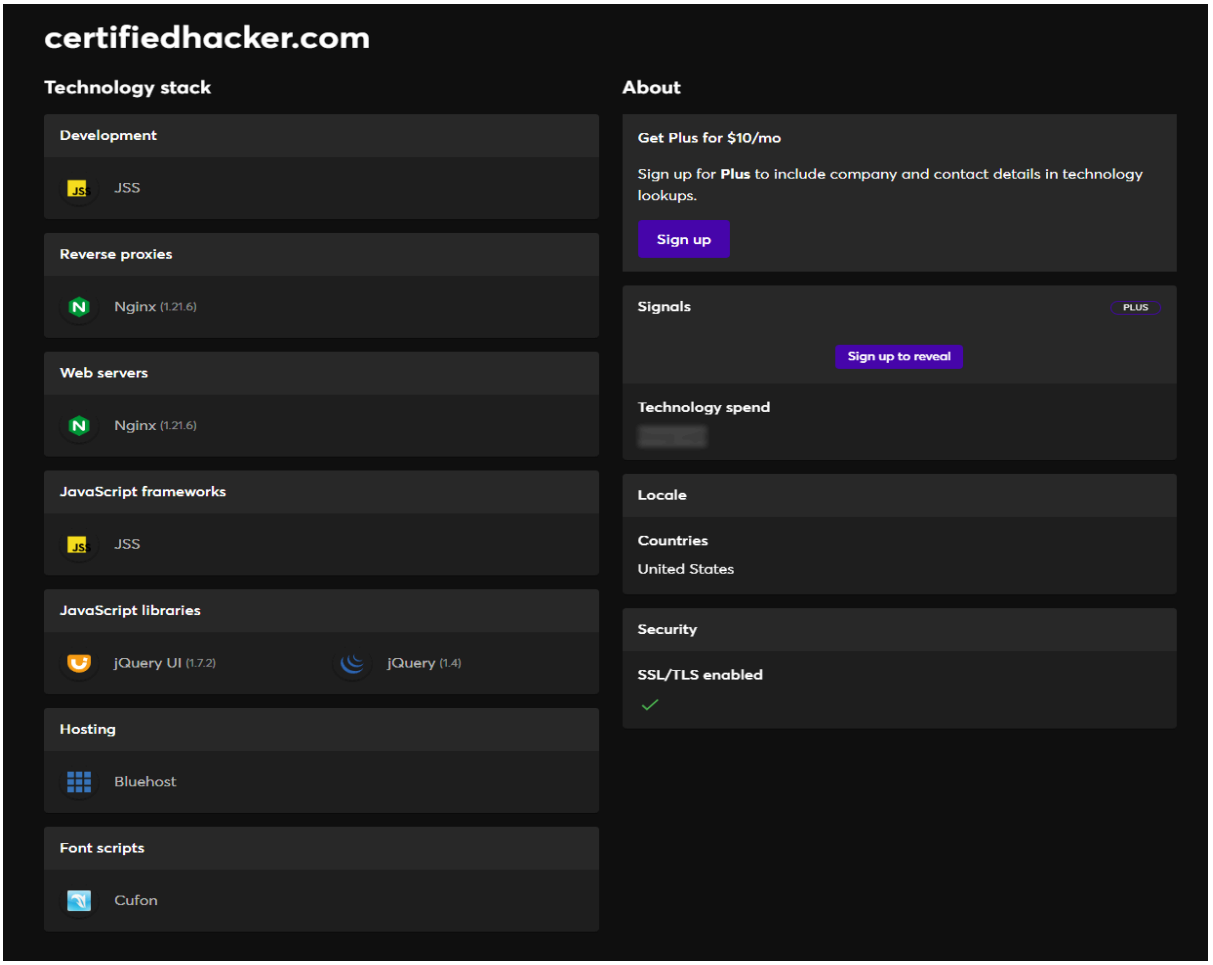
The website has a risk rating of 0/10 where lower is better. It uses a reverse proxy server using nginx and apache. A lot of the personal information of the website admin were found using the tools.All the details like the register address, name, city and email are available in public.The server is advertised in North America but has been located in and around the Utah region. All of the findings are added below along with the screenshot and tool used.

Summary:

I ended up being able to find out a lot of information using straightforward commands and tool searches after assessing the website with several tools. Based on how they are used, a lot of this information that is readily accessible might be regarded as possible vulnerabilities. Following are the tools utilized and the results.



DnsDumpster is a website where we can obtain DNS server and other information by giving in the website link. Through here I found out that the DNS server used here was bluehost. Also identified that all the sub domains used apache server. We also mapped out the server structure in this tool.

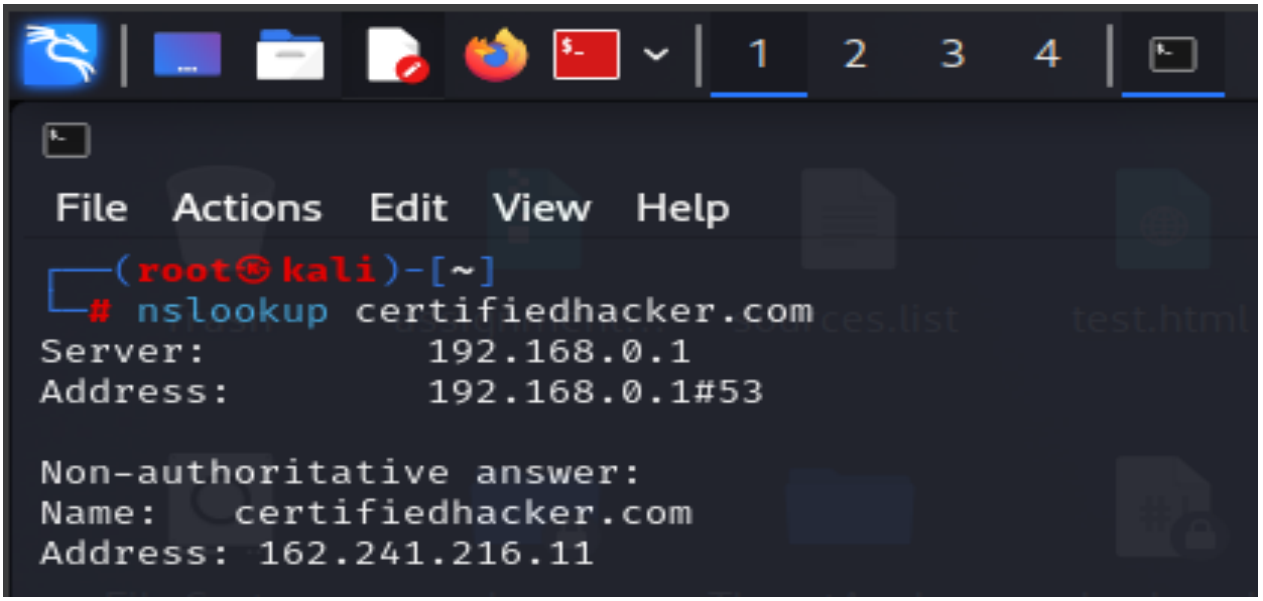


Wappalyzer is a similar tool where we can scan information by entering the website url we are able to pull up information regarding the libraries and framework used in the website.

We discovered that the specified website now has two servers, Apache and nginx, and that Whatruns is a website similar to Wappalyzer that was used to validate the information.

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-08-22T07:58:34Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2024-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq9t994x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: kq9t994x73e@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: kq9t994x73e@networksolutionsprivateregistration.com
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
```

Whois is a linux tool. Using this tool we were able to collect quite a lot of information about the domain owner and the company. For instance we cna see the owner and the companies address, phone no, email and few more potentially exploitable informations.



NsLookup was used to find the server ip and address ip.

Background

Site title	Not Acceptable!	Date first seen	January 2018
Site rank	6246	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	https://certifiedhacker.com	Domain	certifiedhacker.com
Netblock Owner	Unified Layer	Nameserver	ns1.bluehost.com
Hosting company	Newfold Digital	Domain registrar	networksolutions.com
Hosting country	US	Nameserver organisation	whois.domain.com
IPv4 address	162.241.216.11 (VirusTotal)	Organisation	5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems	AS46606	DNS admin	dnsadmin@box5331.bluehost.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	box5331.bluehost.com		

IP delegation

IPv4 address (162.241.216.11)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255	United States	NET162	Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255.255	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer
↳ 162.241.216.11	United States	UNIFIEDLAYER-NETWORK-16	Unified Layer

Netcraft site report and DNS search revealed encryption, certificate and signature information. Which can be used to exploit the website.

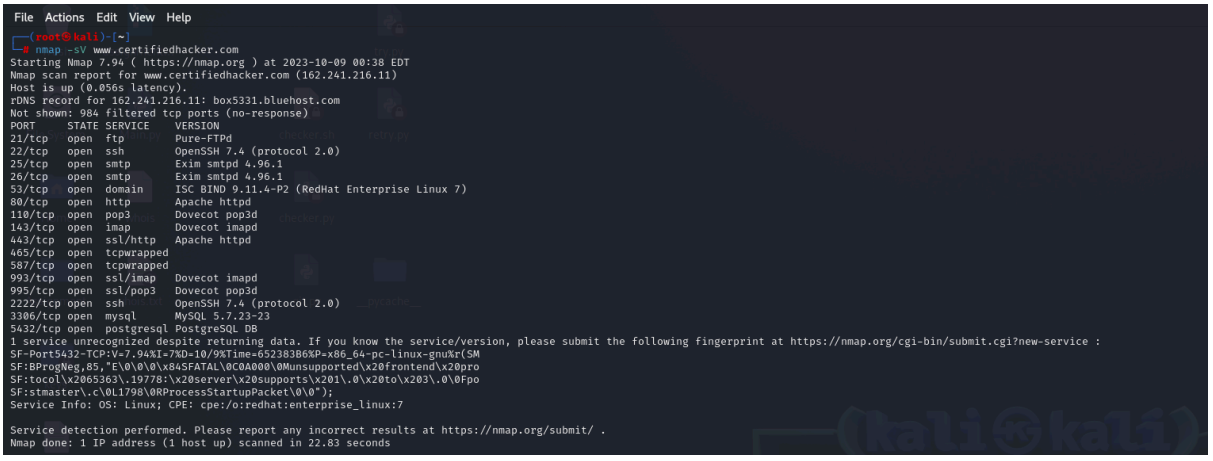
Assignment #3
This is the continuation of the assignment 2 where we are asked to add active recon of the same website (www.certifiedhacker.com) onto the previous report

Active Reconnaissance:
We start with doing a general scan of the web page that resulted in the data of the ip address of the webpage and port/service details of our given webpage.

Nmap, short for "Network Mapper," is a well-known open-source network scanning and security auditing programme. It is applied to network discovery, vulnerability checking, and network security evaluations. Nmap enables you to investigate network hosts, find accessible ports and services, learn more about those services, and even spot potential security holes.

Nmap -sV www.certifiedhacker.com

The Nmap will conduct a thorough scan on the given IP address in an effort to determine the operating system, services, and versions that are present on the target computer. To learn more about the intended system, it might also run a few programmes. Aggressive scanning should only be performed on systems where you have authority to scan with commands because it can be more intrusive and may be picked up by firewalls or intrusion detection systems.
nmap -A 162.241.216.11



Nmap -sC 162.241.216.11

The Nmap scan performed with the command "nmap -sC 162.241.216.11" gives a thorough overview of the services and ports active on the target system (162.241.216.11). The analysis finds that Bluehost is the system's host and that it is using a number of services on the system, including FTP, SSH, DNS, HTTP, POP3, IMAP, HTTPS, SMTP Submission, IMAPS, POP3S, and MySQL. Information about the SSL certificate contains things like the commonName, the subject alternative name, the validity dates, and the TLS randomness. To comprehend the setup and potential security ramifications of the target system, it is helpful to have this precise information.

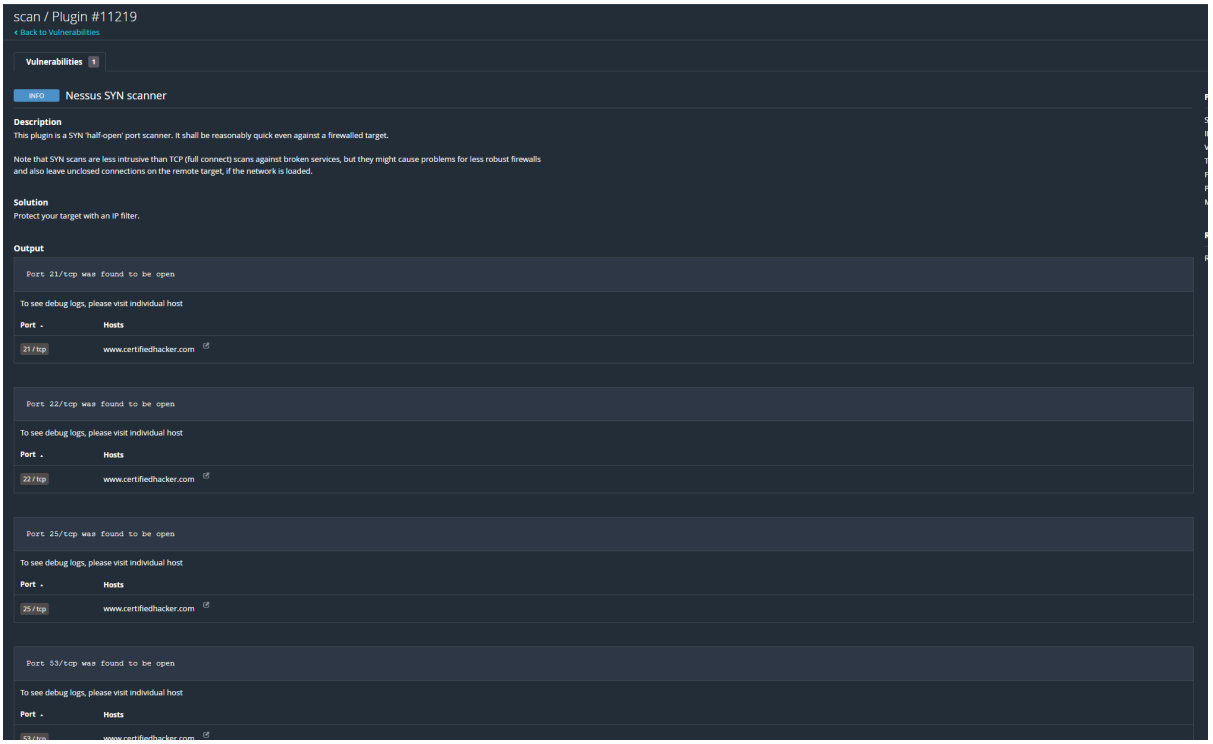
Version Detection can scan certain ports:

Nmap -A 162.241.216.11

The Nmap command "nmap -A -oN output.txt 162.241.216.11" runs a thorough scan on the provided IP address (162.241.216.11) with extra options. As a result, Nmap will conduct a thorough scan on the target IP address when you use this command, including OS detection, version detection, script scanning, and traceroute. The scan's outcomes will be saved in a file with the name "output.txt" in a text format that can be read by humans. The target system's operating system, open ports, services, and any potential vulnerabilities can all be learned about in-depth with the use of this kind of scan. For additional analysis, the stored output file can be inspected.

As noted in content relevant to the open ports found by a Nmap scan, vulnerability databases like CVE, NVD, CWE, and CAPEC can be used to find vulnerabilities connected to it.

Nessus Basic Web Scan:



through the nessus scan we can identify :

- Vulnerabilities that allow unauthorized control or access to sensitive data on a system
- Misconfigurations like open mail relay
- Missing patches
- Use of default passwords, common and blank passwords on some system accounts
- Denials of service (Dos) vulnerabilities

The above found vulnerabilities can be traced back to the CVE Database Some of them are mentioned below for reference:

Port Vulnerabilities:

CVE-ID

CVE-2022-30318 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Honeywell ControlEdge through R151.1 uses Hard-coded Credentials. According to FSCT-2022-0056, there is a Honeywell ControlEdge hardcoded credentials issue. The affected components are characterized as: SSH. The potential impact is: Remote code execution, manipulate configuration, denial of service. The Honeywell ControlEdge PLC and RTU product line exposes an SSH service on port 22/TCP. Login as root to this service is permitted and credentials for the root user are hardcoded without automatically changing them upon first commissioning. The credentials for the SSH service are hardcoded in the firmware. The credentials grant an attacker access to a root shell on the PLC/RTU, allowing for remote code execution, configuration manipulation and denial of service.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-06
- MISC:https://www.forescout.com/blog/

Assigning CNA

MITRE Corporation

Date Record Created

20220506 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20220506)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

CWE-787: Out-of-bounds Write

Weakness ID: 787
Abstraction: Base
Structure: Simple

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

The product writes data past the end, or before the beginning, of the intended buffer.

Extended Description

Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.

Alternate Terms

Memory Corruption: Often used to describe the consequences of writing to memory outside the bounds of a buffer, or to memory that is invalid, when the root cause is something other than a sequential copy of excessive data from a fixed starting location. This may include issues such as incorrect pointer arithmetic, accessing invalid pointers due to incomplete initialization or memory release, etc.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer
ParentOf	V	121	Stack-based Buffer Overflow
ParentOf	V	122	Heap-based Buffer Overflow
ParentOf	B	123	Write-what-where Condition
ParentOf	B	124	Buffer Underwrite ('Buffer Underflow')
CanFollow	B	822	Untrusted Pointer Dereference
CanFollow	B	823	Use of Out-of-range Pointer Offset
CanFollow	B	824	Access of Uninitialized Pointer
CanFollow	B	825	Expired Pointer Dereference

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	C	1218	Memory Buffer Errors

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)
Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)
Relevant to the view "CISQ Data Protection Measures" (CWE-1340)

Port 21

CVE-ID

CVE-2020-10288 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://github.com/aliasrobotics/RVD/issues/3327
- URL:https://github.com/aliasrobotics/RVD/issues/3327

Assigning CNA

Alias Robotics S.L.

Date Record Created

20200310 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200310)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

CVE-ID

CVE-2018-10070 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A vulnerability in MikroTik Version 6.41.4 could allow an unauthenticated remote attacker to exhaust all available CPU and all available RAM by sending a crafted FTP request on port 21 that begins with many '\0' characters, preventing the affected router from accepting new FTP connections. The router will reboot after 10 minutes, logging a "router was rebooted without proper shutdown" message.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:44450
- URL:https://www.exploit-db.com/exploits/44450/
- MISC:http://packetstormsecurity.com/files/147183/MikroTik-6.41.4-Denial-Of-Service.html

Assigning CNA

MITRE Corporation

Date Record Created

20180412 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20180412)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

Port 113

CVE-ID	
CVE-2007-2711	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Stack-based buffer overflow in TinyIdentD 2.2 and earlier allows remote attackers to execute arbitrary code via a long string to TCP port 113.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• BID:23981 • URL:http://www.securityfocus.com/bid/23981 • EXPLOIT-DB:3925 • URL:https://www.exploit-db.com/exploits/3925 • OSVDB:36053 • URL:~~http://osvdb.org/36053~~ (Obsolete source) • SECUNIA:25248 • URL:http://secunia.com/advisories/25248 • VUPEN:ADV-2007-1825 • URL:~~http://www.vupen.com/english/advisories/2007/1825~~ (Obsolete source) • XF:tinyidentd-identification-bo(34298) • URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/34298	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20070515	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20070515)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2018-18388	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
eScan Agent Application (MWAGENT.EXE) 4.0.2.98 in MicroWorld Technologies eScan 14.0 allows remote or local attackers to execute arbitrary commands by sending a carefully crafted payload to TCP port 2222.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:http://blog.escanav.com/2018/11/cve-2018-18388/	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20181016	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20181016)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-2010-0816	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Integer overflow in inetcomm.dll in Microsoft Outlook Express 5.5 SP2, 6, and 6 SP1; Windows Live Mail on Windows XP SP2 and SP3, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7; and Windows Mail on Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote e-mail servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) POP3 or (2) IMAP response, as demonstrated by a certain +OK response on TCP port 110, aka "Outlook Express and Windows Mail Integer Overflow Vulnerability."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:40052
- URL:http://www.securityfocus.com/bid/40052
- BUGTRAQ:20100511 {PRL} Microsoft Windows Outlook Express and Windows Mail Integer Overflow
- URL:http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html
- CERT:TA10-131A
- URL:http://www.us-cert.gov/cas/techalerts/TA10-131A.html
- MISC:http://www.protekresearchlab.com/index.php?option=com_content&view=article&id=13&Itemid=13
- MS:MS10-030
- URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-030
- OVAL:oval:org.mitre.oval:def:6734
- URL:https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6734

Assigning CNA

Microsoft Corporation

Date Record Created

20100302	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20100302)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

Reference:

1.https://cve.mitre.org/