

# **ITMS 543 – Vulnerability Analysis and Control**

**Recon a website**

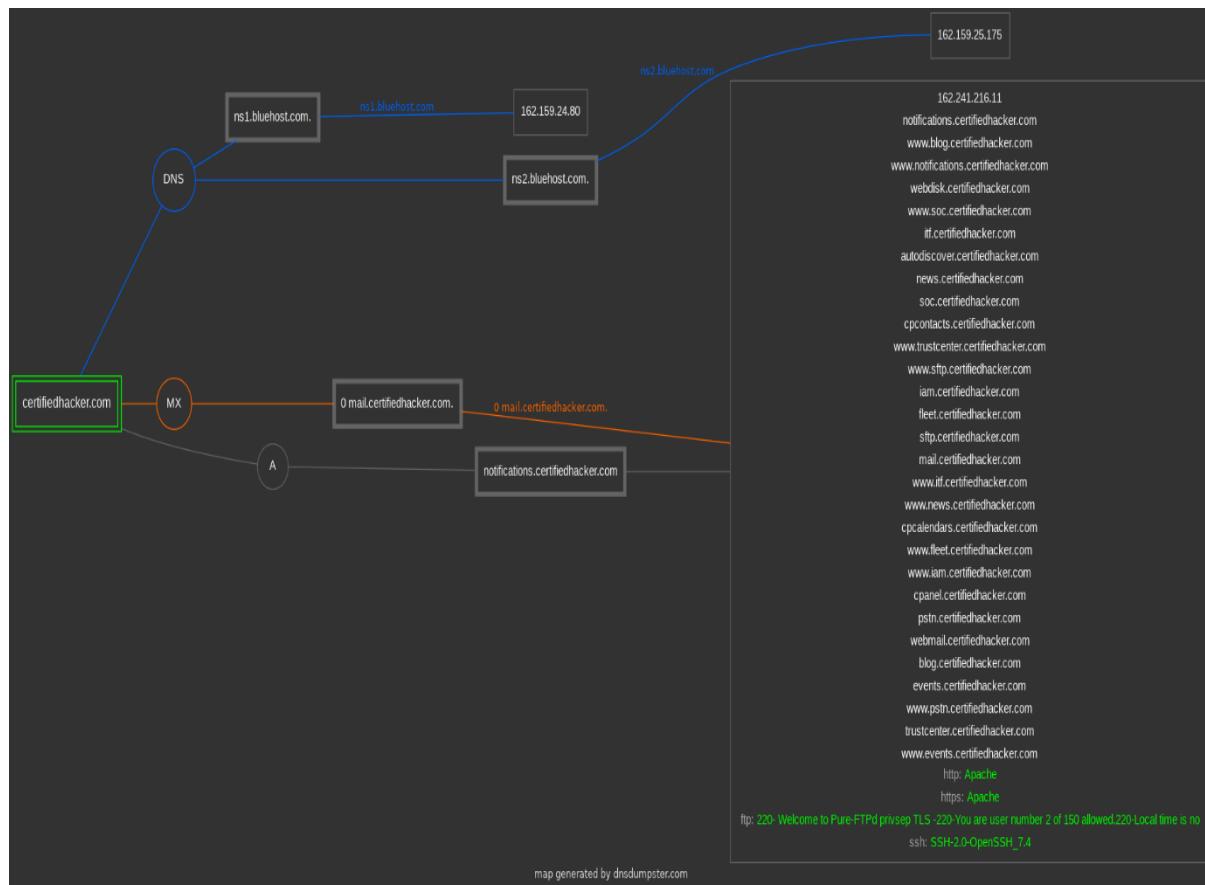
**Rajabinandhan Periyagoundanoor Gopal**

## 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.

The screenshot shows the 'certifiedhacker.com' website's technology stack analysis. On the left, there's a sidebar with various categories: Development (JSS), Reverse proxies (Nginx 1.21.6), Web servers (Nginx 1.21.6), JavaScript frameworks (JSS), JavaScript libraries (jQuery UI 1.7.2, jQuery 1.4), Hosting (Bluehost), and Font scripts (Cufon). On the right, there's an 'About' section with a 'Get Plus for \$10/mo' button, a 'Sign up' button, a 'Signals' section with a 'Sign up to reveal' button, a 'Technology spend' section (partially obscured), a 'Locale' section (United States), a 'Countries' section (United States), and a 'Security' section indicating 'SSL/TLS enabled'.

[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.

The screenshot shows the 'WhatRuns' tool analyzing the website 'certifiedhacker.com'. It lists the following technologies:

- Font Script:** Cufon
- Web Server:** Apache 2.4.18
- Javascript Frameworks:**
  - jQuery 1.4
  - jQuery UI 1.7.2
  - Jquery Easing
  - HoverIntent JS

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 P0 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 P0 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 P0 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 can see the owner and the companies address, phone no, email and few more potentially exploitable informations.

```
(root㉿kali)-[~]
# nslookup certifiedhacker.com
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:  certifiedhacker.com
Address: 162.241.216.11
```

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	<a href="https://certifiedhacker.com">https://certifiedhacker.com</a>	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](http://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](http://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

```
File Actions Edit View Help
[root@kali:~]# nmap -sV www.certifiedhacker.com
Starting Nmap 7.04 ( https://nmap.org ) at 2023-10-09 00:38 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.056s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
25/tcp    open  smtp         Exim Smtpd 4.99.1
26/tcp    open  smtp         Exim Smtpd 4.99.1
33/tcp    open  domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open  http         Apache httpd
110/tcp   open  pop3        Dovecot pop3d
143/tcp   open  imap        Dovecot imapd
443/tcp   open  ssl/http    Apache httpd
465/tcp   open  tcpwrapped
587/tcp   open  tcpwrapped
993/tcp   open  ssl/imap    Dovecot imapd
995/tcp   open  ssl/pop3   Dovecot pop3d
2222/tcp  open  ssh          OpenSSH 7.4 (protocol 2.0)  python_
3306/tcp  open  mysql        MySQL 5.7.23-23
5432/tcp  open  postgresql  PostgreSQL DB
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.94%I=730=10/9%Time=652383B6XP=x86_64-pc-linux-gnu%R(SM
SF:BProgNeg,_85,"E\0\0\0\0\x845FATAL\0C0A000\0Unsupported\x20frontend\x20proto
SF:tocool\x2065363\,,19778:x20server\x20supports\x201\,,\0\x20t\,\x203\,\0\0Fpo
SF:master\,c\0L1798\0RProcessStartupPacket\0\0";
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.83 seconds
```

### 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:

```

root@kali: ~
[+] Port 22/tcp open  ssh  2024-01-07T23:59:59
[+] Port 25/tcp open  smtp  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com Hello: 208-59-147-232.v998.c3-0.mcm-chi-mcm.ll.cable.rcncustomer.com [208.59.147.232], SIZE: 5248000, 808TIME, PIPELINING, PIPECONNECT, AUTH
H: PLAIN LOGIN, STARTTLS, HELO
[*] Connection: AUTH STARTTLS HELO TELNO MAIL RCPT DATA NOOP QUIT RSET HELP
[+] Port 80/tcp open  http   2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[+] Port 110/tcp open  pop3  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 143/tcp open  imap  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 443/tcp open  https  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 993/tcp open  pop3s  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 995/tcp open  imaps  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 2232/tcp open  Ethernet  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 5432/tcp open  postgresql  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 5433/tcp open  mysql  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=mysql.native.password, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
[+] Port 5434/tcp open  postgresql  2024-01-07T23:59:59
[*] Service Info: Host: bnx331.bluehost.com FQDN: bnx331.bluehost.com
[*] SSL/TLS: Subject: commonName=bluehost.com, DNS:bluehost.com
[*] Not valid before: 2024-01-07T23:59:59
[*] Not valid after: 2024-01-07T23:59:59
[*] Service Info: TLS randomness does not represent time
Nmap done: 1 IP address (1 host up) scanned in 39.38 seconds

```

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:

scan / Plugin #11219

[Back to Vulnerabilities](#)

**Vulnerabilities** 1

**INFO** Nessus SYN scanner

**Description**  
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**  
Protect your target with an IP filter.

**Output**

Port 21/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
21/tcp	www.certifiedhacker.com

Port 22/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
22/tcp	www.certifiedhacker.com

Port 25/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
25/tcp	www.certifiedhacker.com

Port 53/tcp was found to be open

To see debug logs, please visit individual host

Port	Hosts
53/tcp	www.certifiedhacker.com

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	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information			
<b>Description</b>				
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.				
<b>References</b>				
<small>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</small> <ul style="list-style-type: none"> <li>• MISC:<a href="https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-06">https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-06</a></li> <li>• MISC:<a href="https://www.forescout.com/blog/">https://www.forescout.com/blog/</a></li> </ul>				
<b>Assigning CNA</b>				
MITRE Corporation				
<b>Date Record Created</b>				
20220506	<small>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.</small>			
<b>Phase (Legacy)</b>				
Assigned (20220506)				
<b>Votes (Legacy)</b>				
<b>Comments (Legacy)</b>				
<b>Proposed (Legacy)</b>				
N/A				

## CWE-787: Out-of-bounds Write

<b>Weakness ID: 787</b>	Abstraction: Base																																				
	Structure: Simple																																				
<small>View customized information:</small> <a href="#">Conceptual</a> <a href="#">Operational</a> <a href="#">Mapping Friendly</a> <a href="#">Complete</a> <a href="#">Custom</a>																																					
<b>▼ Description</b> The product writes data past the end, or before the beginning, of the intended buffer.																																					
<b>▼ Extended Description</b> 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.																																					
<b>▼ Alternate Terms</b> <b>Memory Corruption:</b> 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.																																					
<b>▼ Relationships</b> <ul style="list-style-type: none"> <li><b>Relevant to the view "Research Concepts" (CWE-1000)</b> <table border="1"> <thead> <tr> <th>Nature</th> <th>Type ID</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>ChildOf</td> <td>119</td> <td><a href="#">Improper Restriction of Operations within the Bounds of a Memory Buffer</a></td> </tr> <tr> <td>ParentOf</td> <td>121</td> <td><a href="#">Stack-based Buffer Overflow</a></td> </tr> <tr> <td>ParentOf</td> <td>122</td> <td><a href="#">Heap-based Buffer Overflow</a></td> </tr> <tr> <td>ParentOf</td> <td>123</td> <td><a href="#">Write-what-where Condition</a></td> </tr> <tr> <td>ParentOf</td> <td>124</td> <td><a href="#">Buffer Underwrite ('Buffer Underflow')</a></td> </tr> <tr> <td>CanFollow</td> <td>822</td> <td><a href="#">Untrusted Pointer Dereference</a></td> </tr> <tr> <td>CanFollow</td> <td>823</td> <td><a href="#">Use of Out-of-range Pointer Offset</a></td> </tr> <tr> <td>CanFollow</td> <td>824</td> <td><a href="#">Access of Uninitialized Pointer</a></td> </tr> <tr> <td>CanFollow</td> <td>825</td> <td><a href="#">Expired Pointer Dereference</a></td> </tr> </tbody> </table> </li> <li><b>Relevant to the view "Software Development" (CWE-699)</b> <table border="1"> <thead> <tr> <th>Nature</th> <th>Type ID</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>MemberOf</td> <td>1218</td> <td><a href="#">Memory Buffer Errors</a></td> </tr> </tbody> </table> </li> </ul>		Nature	Type ID	Name	ChildOf	119	<a href="#">Improper Restriction of Operations within the Bounds of a Memory Buffer</a>	ParentOf	121	<a href="#">Stack-based Buffer Overflow</a>	ParentOf	122	<a href="#">Heap-based Buffer Overflow</a>	ParentOf	123	<a href="#">Write-what-where Condition</a>	ParentOf	124	<a href="#">Buffer Underwrite ('Buffer Underflow')</a>	CanFollow	822	<a href="#">Untrusted Pointer Dereference</a>	CanFollow	823	<a href="#">Use of Out-of-range Pointer Offset</a>	CanFollow	824	<a href="#">Access of Uninitialized Pointer</a>	CanFollow	825	<a href="#">Expired Pointer Dereference</a>	Nature	Type ID	Name	MemberOf	1218	<a href="#">Memory Buffer Errors</a>
Nature	Type ID	Name																																			
ChildOf	119	<a href="#">Improper Restriction of Operations within the Bounds of a Memory Buffer</a>																																			
ParentOf	121	<a href="#">Stack-based Buffer Overflow</a>																																			
ParentOf	122	<a href="#">Heap-based Buffer Overflow</a>																																			
ParentOf	123	<a href="#">Write-what-where Condition</a>																																			
ParentOf	124	<a href="#">Buffer Underwrite ('Buffer Underflow')</a>																																			
CanFollow	822	<a href="#">Untrusted Pointer Dereference</a>																																			
CanFollow	823	<a href="#">Use of Out-of-range Pointer Offset</a>																																			
CanFollow	824	<a href="#">Access of Uninitialized Pointer</a>																																			
CanFollow	825	<a href="#">Expired Pointer Dereference</a>																																			
Nature	Type ID	Name																																			
MemberOf	1218	<a href="#">Memory Buffer Errors</a>																																			
<ul style="list-style-type: none"> <li><b>Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)</b></li> <li><b>Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)</b></li> <li><b>Relevant to the view "CISQ Data Protection Measures" (CWE-1340)</b></li> </ul>																																					

## Port 21

CVE-ID	
<b>CVE-2020-10288</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • 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	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> <li>CONFIRM:<a href="https://github.com/aliasrobotics/RVD/issues/3327">https://github.com/aliasrobotics/RVD/issues/3327</a></li> <li>URL:<a href="https://github.com/aliasrobotics/RVD/issues/3327">https://github.com/aliasrobotics/RVD/issues/3327</a></li> </ul>	
Assigning CNA	
Alias Robotics S.L.	
Date Record Created	
<b>20200310</b>	Disclaimer: The <a href="#">record creation date</a> 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 <a href="#">CVE List</a> , which provides common identifiers for publicly known cybersecurity vulnerabilities.	

CVE-ID	
<b>CVE-2018-10070</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • 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	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> <li>EXPLOIT-DB:44450</li> <li>URL:<a href="https://www.exploit-db.com/exploits/44450/">https://www.exploit-db.com/exploits/44450/</a></li> <li>MISC:<a href="http://packetstormsecurity.com/files/147183/MikroTik-6.41.4-Denial-Of-Service.html">http://packetstormsecurity.com/files/147183/MikroTik-6.41.4-Denial-Of-Service.html</a></li> </ul>	
Assigning CNA	
MITRE Corporation	
Date Record Created	
<b>20180412</b>	Disclaimer: The <a href="#">record creation date</a> 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 <a href="#">CVE List</a> , which provides common identifiers for publicly known cybersecurity vulnerabilities.	

## Port 113

<b>CVE-ID</b>	
<b>CVE-2007-2711</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
<b>Description</b>	
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.	
<b>References</b>	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> <li>• BID:23981</li> <li>• URL:<a href="http://www.securityfocus.com/bid/23981">http://www.securityfocus.com/bid/23981</a></li> <li>• EXPLOIT-DB:3925</li> <li>• URL:<a href="https://www.exploit-db.com/exploits/3925">https://www.exploit-db.com/exploits/3925</a></li> <li>• OSVDB:36053</li> <li>• URL:<a href="http://osvdb.org/36053">http://osvdb.org/36053</a> (Obsolete source)</li> <li>• SECUNIA:25248</li> <li>• URL:<a href="http://secunia.com/advisories/25248">http://secunia.com/advisories/25248</a></li> <li>• VUPEN:ADV-2007-1825</li> <li>• URL:<a href="http://www.vupen.com/english/advisories/2007/1825">http://www.vupen.com/english/advisories/2007/1825</a> (Obsolete source)</li> <li>• XF:tinyidentd-identification-bo(34298)</li> <li>• URL:<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/34298">https://exchange.xforce.ibmcloud.com/vulnerabilities/34298</a></li> </ul>	
<b>Assigning CNA</b>	
MITRE Corporation	
<b>Date Record Created</b>	
<b>20070515</b>	Disclaimer: The <a href="#">record creation date</a> 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.
<b>Phase (Legacy)</b>	
Assigned (20070515)	
<b>Votes (Legacy)</b>	
<b>Comments (Legacy)</b>	
<b>Proposed (Legacy)</b>	
N/A	
<b>CVE-ID</b>	
<b>CVE-2018-18388</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
<b>Description</b>	
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.	
<b>References</b>	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> <li>• CONFIRM:<a href="http://blog.escanav.com/2018/11/cve-2018-18388/">http://blog.escanav.com/2018/11/cve-2018-18388/</a></li> </ul>	
<b>Assigning CNA</b>	
MITRE Corporation	
<b>Date Record Created</b>	
<b>20181016</b>	Disclaimer: The <a href="#">record creation date</a> 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.
<b>Phase (Legacy)</b>	
Assigned (20181016)	
<b>Votes (Legacy)</b>	
<b>Comments (Legacy)</b>	
<b>Proposed (Legacy)</b>	
N/A	

<b>CVE-2010-0816</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a>
<b>Description</b>	
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."	
<b>References</b>	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> <li>• BID:40052</li> <li>• URL:<a href="http://www.securityfocus.com/bid/40052">http://www.securityfocus.com/bid/40052</a></li> <li>• BUGTRAQ:20100511 {PRL} Microsoft Windows Outlook Express and Windows Mail Integer Overflow</li> <li>• URL:<a href="http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html">http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html</a></li> <li>• CERT:TA10-131A</li> <li>• URL:<a href="http://www.us-cert.gov/cas/techalerts/TA10-131A.html">http://www.us-cert.gov/cas/techalerts/TA10-131A.html</a></li> <li>• MISC:<a href="http://www.protekresearchlab.com/index.php?option=com_content&amp;view=article&amp;id=13&amp;Itemid=13">http://www.protekresearchlab.com/index.php?option=com_content&amp;view=article&amp;id=13&amp;Itemid=13</a></li> <li>• MS:MS10-030</li> <li>• URL:<a href="https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-030">https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-030</a></li> <li>• OVAL:oval:org.mitre.oval:def:6734</li> <li>• URL:<a href="https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6734">https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6734</a></li> </ul>	
<b>Assigning CNA</b>	
Microsoft Corporation	
<b>Date Record Created</b>	
20100302	Disclaimer: The <a href="#">record creation date</a> 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.
<b>Phase (Legacy)</b>	
Assigned (20100302)	
<b>Votes (Legacy)</b>	
<b>Comments (Legacy)</b>	
<b>Proposed (Legacy)</b>	
N/A	

**Reference:**

- 1.** <https://cve.mitre.org/>