JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

Product ID: JCSA-20240918-001

September 18, 2024

People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations

Summary

The Federal Bureau of Investigation (FBI), Cyber National Mission Force (CNMF), and National Security Agency (NSA) assess that People's Republic of China (PRC)-linked cyber actors have compromised thousands of Internet-connected devices, including small office/home office (SOHO) routers, firewalls, network-attached storage (NAS) and Internet of Things (IoT) devices with the goal of creating a network of compromised nodes (a "botnet") positioned for malicious activity. The actors may then use the botnet as a proxy to conceal their identities while deploying distributed denial of service (DDoS) attacks or compromising targeted U.S. networks.

Integrity Technology Group (Integrity Tech), a PRC-based company, has controlled and managed a botnet active since mid-2021. The botnet has regularly maintained between tens to hundreds of thousands of compromised devices. As of June 2024, the botnet consisted of over 260,000 devices. Victim devices which are part of the botnet have been observed in North America, South America, Europe, Africa, Southeast Asia and Australia.

While devices aged beyond their end-of-life dates are known to be more vulnerable to intrusion, many of the compromised devices in the Integrity Tech-controlled botnet are likely still supported by their respective vendors.

FBI, CNMF, NSA, and allied partners are releasing this Joint Cyber Security Advisory to highlight the threat posed by these actors and their botnet activity and to encourage exposed device vendors, owners, and operators to update and secure their devices from being compromised and joining the botnet. Network defenders are advised to follow the guidance in the mitigations section to protect against the PRC-linked cyber actors' botnet activity. Cyber security companies can also leverage the information in this advisory to assist with identifying malicious activity and reducing the number of devices present in botnets worldwide.

For additional information, see U.S. Department of Justice (DOJ) press release.

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

Technical Details

Attribution

Integrity Tech is a company based in the PRC with links to the PRC government. Integrity Tech has used China Unicom Beijing Province Network IP addresses to control and manage the botnet described in this advisory.

In addition to managing the botnet, these same China Unicom Beijing Province Network IP addresses were used to access other operational infrastructure employed in computer intrusion activities against U.S. victims. FBI has engaged with multiple U.S. victims of these computer intrusions and found activity consistent with the tactics, techniques, and infrastructure associated with the cyber threat group known publicly as Flax Typhoon, RedJuliett, and Ethereal Panda.

Note: Cybersecurity companies have different methods of tracking and attributing cyber actors, and these may not be a 1:1 correlation to the U.S. Government's methodology and understanding for all activity related to these groupings.

Botnet Command and Control

As with similar botnets, this botnet infrastructure is comprised of a network of devices, known as "bots," which are infected with a type of malware that provides threat actors with unauthorized remote access. A functioning botnet can be used for a variety of purposes, including malware delivery, distributed denial of service (DDoS) attacks, or routing nefarious Internet traffic.

The botnet uses the Mirai family of malware, designed to hijack IoT devices such as webcams, DVRs, IP cameras, and routers running Linux-based operating systems. The Mirai source code was posted publicly on the Internet in 2016, resulting in other hackers creating their own botnets based on the malware. Since that time, various Mirai botnets have been used to conduct DDoS and other malicious activities against victim entities within the U.S.

The investigated botnet's customized Mirai malware is a component of a system that automates the compromise of a variety of devices. To recruit a new "bot," the botnet system first compromises an Internet-connected device using one of a variety of known vulnerability exploits (see Appendix B: Observed CVEs). Post-compromise, the victim device executes a Mirai-based malware payload from a remote server. Once executed, the payload starts processes on the device to establish a connection with a command-and-control (C2) server using Transport Layer Security (TLS) on port 443. The processes gather system information from the infected device, including but not limited to the operating system version and processor, memory and bandwidth details to send to the C2 server for enumeration purposes. The malware also makes requests to "c.speedtest.net," likely to gather additional Internet connection details. Some malware payloads were self-deleting to evade detection.

A variety of subdomains of "w8510.com" were linked to the botnet's C2 servers. As of September 2024, investigators identified over 80 subdomains associated with w8510.com (see Appendix A: Indicators of Compromise).

Botnet Management

A tier of upstream management servers using TCP port 34125 manage the botnet's C2 servers. These management servers host a MySQL database which stored information used for the control of the botnet. As of June 2024, this database contained over 1.2 million records of compromised devices, including over 385,000 unique U.S. victim devices, both previously and actively exploited.

The management servers hosted an application known as "Sparrow," which allows users to interact with the botnet. The actors used specific IP addresses registered to China Unicom Beijing Province Network to access this application, including the same IP addresses previously used by Flax Typhoon to access the systems used in computer intrusion activities against U.S.-based victims.

The code for the Sparrow application, stored within a Git repository, defines functions that allow registered users to manage and control the botnet and C2 servers, sending tasks to victim devices including DDoS and exploitation commands to grow the botnet. Sparrow also contains functionality providing device vulnerability information to users. A subcomponent called "vulnerability arsenal" also allows users to exploit traditional computer networks through the victim devices in the botnet.

Compromised Device Distribution

The following tables approximate the count of devices compromised by the botnet system as of June 2024, by location and by processor architecture. There were at least 50 different Linux operating system versions found among botnet nodes. Based on the operating system versions of the nodes, infected systems include devices that ceased receiving support as early as 2016 to devices that are currently supported. Affected devices were running Linux kernel versions 2.6 through 5.4.

Table 1: Botnet devices per country

Country	Node Count	Percentage
United States	126,000	47.9%
Vietnam	21,100	8.0%
Germany	18,900	7.2%
Romania	9,600	3.7%
Hong Kong	9,400	3.6%
Canada	9,200	3.5%
South Africa	9,000	3.4%
United Kingdom	8,500	3.2%
India	5,800	2.2%
France	5,600	2.1%
Bangladesh	4,100	1.6%
Italy	4,000	1.5%
Lithuania	3,300	1.3%
Albania	2,800	1.1%
Netherlands	2,700	1.0%
China	2,600	1.0%
Australia	2,400	0.9%
Poland	2,100	0.8%
Spain	2,000	0.8%

Table 2: Botnet devices per continent

Continent	Node Count	Percentage
North America	135,300	51.3%
Europe	65,600	24.9%
Asia	50,400	19.1%
Africa	9,200	3.5%
Oceania	2,400	0.9%
South America	800	0.3%

Table 3: Botnet devices by processor architecture

Processor Architecture	Node Count	Percentage
x86	236,000	89.2%
MIPS	21,400	8.1%
ARM	3,900	1.5%
x86_64	1,900	0.7%
MIPSEL	1,400	0.5%

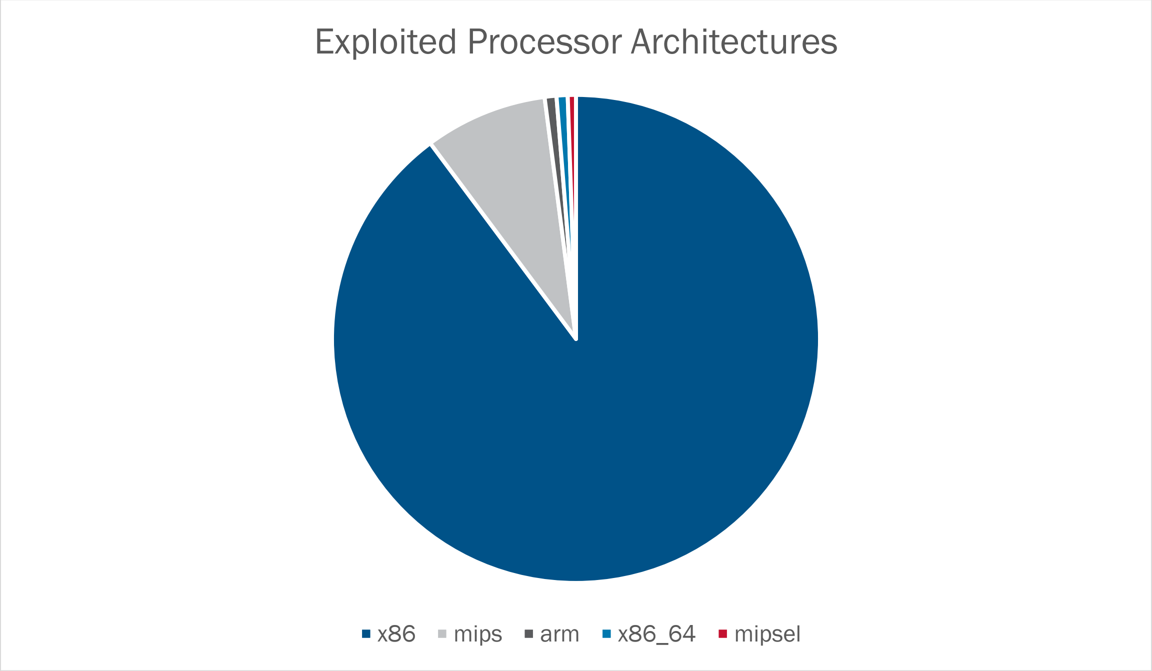

Figure 1: Exploited processor architectures chart

Recommended Mitigations

The FBI recommends network defenders take the following actions to mitigate threats posed by adversaries attempting to use botnets for malicious cyber activity. The following guidance applies both to preventing IoT devices from becoming part of a botnet, as well as to defending networks from botnets already in operation.

- **Disable unused services and ports** such as automatic configuration, remote access or file sharing protocols. Routers and IoT devices may provide features such as Universal Plug and Play (UPnP), remote management options, and file sharing services, which threat actors may abuse to gain initial access or to spread malware to other networked devices. Disable these features if not needed.
- **Implement network segmentation** to ensure IoT devices within a larger network pose known, limited, and tolerable risks. Use the principle of least privilege to provide devices with just enough connectivity needed to perform their intended function.
- **Monitor for high network traffic volume.** Since DDoS attacks originating from botnets may at first appear similar to normal traffic, it is critical for organizations to define, monitor and prepare for abnormal traffic volumes. Monitoring is possible via firewalls or intrusion detection systems. Some network solutions such as proxies may mitigate DDoS incidents.
- **Apply patches and updates**, including software and firmware updates. Regular patching mitigates many high-risk security vulnerabilities. If available, take advantage of automatic update channels from trusted network locations. Do not trust email messages claiming to provide software updates as attachments or via links to untrusted websites.
- **Replace default passwords with strong passwords.** Many IoT products implement a device administration password in addition to other account passwords. Ensure all passwords are changed from their defaults, using a strong password policy. If possible, disable password hints.
- **Plan for device reboots.** Rebooting a device terminates all running processes, which may remove

specific types of malware, such as “fileless” malware that runs in the host’s memory. As a reboot may disrupt legitimate activity, users may need to prepare for service interruptions. Some devices provide scheduled reboot features, enabling reboots to occur at preferred times. If a compromised device fails to respond to reboot commands issued remotely, reboot physically.

- **Replace end-of-life equipment** with devices that remain in respective vendor support plans.

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The authoring organizations do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring organizations.

Version History

September 18, 2024: Initial version.

Appendix A: Indicators of Compromise

The following listed domain names were observed subdomains of “w8510.com,” the observed command and control system domain.

Table 4: List of w8510.com subdomains

Domain	IP Address	Last Seen
acqv.w8510.com	208.85.16.100	8/29/2024
aewreiuicajo.w8510.com	45.77.231.209	9/1/2024
apdfhhjcxcb.w8510.com	139.180.137.219	8/31/2024
asdvxzzxvza.w8510.com	45.135.117.131	9/3/2024
awbpxtpi.w8510.com	155.138.151.225	9/3/2024
bzbatflwb.w8510.com	45.77.231.209	9/3/2024
cansqra.w8510.com	222.186.48.201	8/22/2023
canwtrow.w8510.com	222.186.48.204	10/7/2023
cccasdqawer.w8510.com	92.38.185.45	9/3/2024
ccccasdasdq.w8510.com	85.90.216.115	9/3/2024
cccvbsdfsdf.w8510.com	195.234.62.197	9/3/2024
ccmmkmnkna.w8510.com	85.90.216.69	9/3/2024
cpooooim.w8510.com	85.90.216.110	9/3/2024
dftiscasdwe.w8510.com	207.148.122.69	9/2/2024
dvasrdftqgqg.w8510.com	45.10.58.129	9/3/2024
iiiiopasdfcasd.w8510.com	92.38.185.46	9/3/2024
iikljhg.w8510.com	85.90.216.116	9/3/2024
iuyrdfvv.w8510.com	45.10.58.133	9/3/2024
iyasdasfda.w8510.com	195.234.62.184	9/1/2024

kliscjaisdjhi.w8510.com	149.248.51.22	9/4/2024
lkljjhidjaiwd.w8510.com	37.61.229.15	9/3/2024
lkopiyut.w8510.com	5.181.27.219	9/3/2024
lyblqwesfawe.w8510.com	78.141.238.97	8/28/2024
mjiudwajhkf.w8510.com	45.77.231.209	9/3/2024
mmjkjiu.w8510.com	92.38.185.43	9/3/2024
mmnajsdh.w8510.com	37.9.35.91	9/1/2024
mnbghjj.w8510.com	45.92.70.71	9/2/2024
ocmnusdjdik.w8510.com	139.180.137.219	9/2/2024
oiuiasdads.w8510.com	195.234.62.188	9/3/2024
plllkkoasdko.w8510.com	195.234.62.198	9/3/2024
poiaqqrjk.w8510.com	195.234.62.192	9/3/2024
pojkkaka.w8510.com	45.10.58.130	9/3/2024
poooooiioasd.w8510.com	37.61.229.17	9/3/2024
ppppoiiua.w8510.com	92.38.185.44	9/3/2024
qacassdfawemp.w8510.com	155.138.133.56	9/4/2024
qmmklou.w8510.com	45.92.70.68	9/3/2024
qwertdvvaaz.w8510.com	45.135.117.136	9/3/2024
ssacawfafwa.w8510.com	45.10.58.132	9/3/2024
testate.w8510.com	207.148.68.131	8/30/2024
testateone.w8510.com	108.61.177.81	9/3/2024
tuisasdcxzd.w8510.com	78.141.238.97	8/29/2024
uqooapp.w8510.com	85.90.216.112	9/3/2024

uuiyiyasd.w8510.com	92.38.185.47	9/3/2024
wmllxwkg.w8510.com	45.77.231.209	9/3/2024
zasdfgasd.w8510.com	65.20.97.251	9/3/2024
zda4g4.w8510.com	91.216.190.154	9/3/2024
zda896.w8510.com	45.13.199.152	9/3/2024
zda9ol.w8510.com	91.216.190.247	9/3/2024
zdaaac.w8510.com	5.181.27.6	9/1/2024
zdaasdafq.w8510.com	45.80.215.156	9/3/2024
zdabnv.w8510.com	23.236.68.161	9/3/2024
zdacasc.w8510.com	45.80.215.150	9/2/2024
zdacasdc.w8510.com	195.234.62.19	9/3/2024
zdacawca.w8510.com	45.13.199.84	8/28/2024
zdacccz.w8510.com	5.181.27.21	8/23/2024
zdacppao.w8510.com	45.13.199.140	9/2/2024
zdacscswc.w8510.com	89.44.198.195	8/30/2024
zdacvb.w8510.com	23.236.69.110	9/3/2024
zdacvbzzs.w8510.com	45.13.199.104	9/3/2024
zdacwaca.w8510.com	45.80.215.153	9/2/2024
zdacwrf.w8510.com	45.92.70.111	9/1/2024
zdacx46.w8510.com	23.236.68.213	8/24/2024
zdacxdawdas.w8510.com	45.13.199.45	8/28/2024
zdacxzd.w8510.com	89.44.198.200	9/2/2024
zdaczcaaw.w8510.com	45.80.215.151	8/30/2024

zdaczcvs1.w8510.com	92.38.176.156	7/22/2024
zdaczsc.w8510.com	45.92.70.113	8/13/2024
zdaczvs.w8510.com	45.80.215.149	9/2/2024
zdaczxc1.w8510.com	23.236.68.193	9/4/2024
zdafaa.w8510.com	91.216.190.74	9/3/2024
zdamkl.w8510.com	5.181.27.19	9/2/2024
zdaplm.w8510.com	45.92.70.115	8/28/2024
zdapoi.w8510.com	45.80.215.152	9/2/2024
zdapoq.w8510.com	45.13.199.96	9/2/2024
zdaqggh.w8510.com	23.236.69.82	9/1/2024
zdaqwfasf.w8510.com	45.92.70.112	8/31/2024
zdavva.w8510.com	195.234.62.18	8/27/2024
zdaxcxzc.w8510.com	91.216.190.80	9/2/2024
zdazzz.w8510.com	45.13.199.207	8/29/2024
zdcacaw.w8510.com	45.80.215.155	8/31/2024
zdcawca.w8510.com	45.80.215.154	8/25/2024
zdpoa.w8510.com	89.44.198.254	9/3/2024
zdpog.w8510.com	45.80.215.47	9/3/2024
zdqqqwe.w8510.com	91.216.190.2	9/2/2024
zdzvbs.w8510.com	23.236.68.229	9/3/2024
zzxnjiq.w8510.com	85.90.216.111	9/3/2024
zzzcmsq.w8510.com	5.45.184.68	9/2/2024

Appendix B: Observed CVEs

Integrity Tech relied on the following vulnerabilities to acquire new botnet victims and allow botnet users to exploit further victims through the compromised botnet devices.

Table 5: CVEs exploited to add devices to botnet and exploit further victims

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2024-5217	ServiceNow	Now Platform	Washington DC, Vancouver, and earlier Now Platform releases	RCE
CVE-2024-4577	PHP Group	PHP	PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows	OS command injection
CVE-2024-29973	Zyxel	NAS326 NAS542	NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0	OS command injection
CVE-2024-29269	Telesquare	TLR-2005Ksh	1.0.0 and 1.1.4	Arbitrary system commands
CVE-2024-21762	Fortinet	FortiOS	FortiOS 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17,	RCE
		FortiProxy	FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7	
CVE-2023-50386	Apache	Solr	6.0.0 through 8.11.2, 9.0.0 before 9.4.1	Unrestricted file upload
CVE-2023-47218	QNAP	QTS QuTS hero QuTScloud	QTS 5.1.x before 5.1.5.2645 build 20240116, QuTS hero h5.1.x before h5.1.5.2647 build 20240118, QuTScloud c5.x before c5.1.5.2651	OS command injection

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2023-46747	F5	F5 Big-IP	Big-IP (all modules) 17.1.0-17.1., 16.1.0-16.1.4, 15.1.0-15.1.10, 14.1.0-14.1.5,13.1.0-13.1.5	Authentication bypass
CVE-2023-46604	Apache	Apache ActiveMQ	Before 5.15.16, 5.16.7, 5.17.6, or 5.18.3	RCE
CVE-2023-43478	Telstra	Smart Modem Gen 2	Firmware versions before 0.18.15r	Code execution as root
CVE-2023-4166	Tongda OA	Tongda2000	11.10	SQL injection
CVE-2023-38646	Metabase	Metabase and Metabase Enterprise	Metabase before 0.46.6.1, Metabase Enterprise before 1.46.6.1	Arbitrary command execution
CVE-2023-3852	OpenRapid	Yuque RapidCMS	Up to version 1.3.1	Arbitrary file upload
CVE-2023-38035	Ivanti	MobileIron Sentry (MICS Admin Portal)	9.18.0 and below	Authentication bypass
CVE-2023-37582	Apache	RocketMQ	5.1.1	Remote command execution
CVE-2023-36844	Juniper	Juniper Junos	20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4	PHP external variable modification
CVE-2023-36542	Apache	Apache NiFi	0.0.2 through 1.22.0	Code injection
CVE-2023-35885	CloudPanel	CloudPanel 2	Before 2.3.1	Insecure file-manager cookie authentication
CVE-2023-35843	NocoDB	NocoDB	Through 0.106.0 (or 0.109.1)	Path traversal
CVE-2023-3519	Citrix	Netscaler Gateway, Application Delivery Controller (ADC)	12.1-NDcPP before 55.297, 12.1-FIPS before 55.297, 13.1-FIPS before 37.159, 13.0 before 91.13, 13.1 before 49.13	Unauthenticated remote code execution
CVE-2023-35081	Ivanti	Endpoint Manager Mobile (EPMM)	11.10x<11.10.0.3, 11.9x<11.91.2, and 11.8<11.8.12	Path traversal
CVE-2023-34960	Chamilo	Chamilo	v1.11.* up to v1.11.18	Command injection
CVE-2023-34598	Gibbonedu	Gibbon	25.0.00	Local File Inclusion (LFI) vulnerability

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2023-3368	Chamilo	Chamilo LMS	<= v1.11.20	Command injection leading to remote code execution (RCE) Bypass of CVE-2023-34960
CVE-2023-33510	WordPress	Jeecg P3 Bix Chat	Jeecg P3 Biz Chat Project Jeecg P3 Biz Chat 1.0.5	Allows remote attackers to read arbitrary files
CVE-2023-30799	MikroTik	MikroTik RouterOS	Stable before 6.49.7 and long-term through 6.48.6	Privilege escalation
CVE-2023-28771	Zyxel	ZyWALL/USG series	ZyWALL/USG ZLD 4.60 to 4.73, VPN ZLD 4.60 to 5.35, USG FLEX ZLD 4.60 to 5.35, ATP ZLD 4.60 to 5.35	OS command injection
CVE-2023-28365	Ubiquiti	UI UniFi	7.3.83 and earlier	Backup file vulnerability
CVE-2023-27997	Fortinet	FortiOS	FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below	Buffer overflow
		FortiProxy	FortiProxy 7.2.3 and below, 7.0.9 and below, 2.0.12 and below, 1.2 all versions, 1.1 all versions	
CVE-2023-27524	Apache	Apache Superset	Versions up to and including 2.0.1.	Authenticate and access unauthorized resources
CVE-2023-26469	Jorani	Jorani	1.0.0	Path traversal to RCE
CVE-2023-25690	Apache	Apache HTTP Server	2.4.0 through 2.4.55	HTTP request smuggling
CVE-2023-24229	DrayTek	Vigor2960	Firmware v1.5.1.4 No longer supported by maintainer	Command injection
CVE-2023-23333	Contec	SolarView Compact	Firmware through 6.00	Command injection
CVE-2023-22527	Confluence	Data Center and Server	< 8.5.5 (LTS) < 8.7.2 (Data Center Only)	Template injection leading to RCE

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2023-22515	Confluence	Data Center and Server	>=8.0.0, >= 8.1.0, >=8.2.0, >=8.30 to <8.3.3, >=8.4.0 to <8.4.3, >=8.5.0 to <8.5.2	Privilege escalation
CVE-2022-42475	Fortinet	FortiOS	FortiOS SSL-VPN 7.2.0 through 7.22, 7.00 through 7.0.8, 6.4.0 through 6.4.10, 6.2.0 through 6.211, 6.0.15 and earlier	Buffer overflow
		FortiProxy	FortiProxy SSL VPN 7.2.0 through 7.2.1, 7.0.7 and earlier.	
CVE-2022-40881	Contec	SolarView Compact	Firmware 6.00	Command injection
CVE-2022-3590	WordPress	WordPress	WordPress 4.1	Unauthenticated blind SSRF in the pingback feature
CVE-2022-31814	Netgate	pfSense pfBlockerNG	Through 2.1.4_26	OS command injection
CVE-2022-30525	Zyxel	USG FLEX, ATP, and VPN series firmware	USG FLEX 100(W)/200/500/700 ZLD 5.00 through 5.21 Patch 1, USG FLEX 50(W)/USG20(W)-VPN ZLD 5.10 through 5.21 Patch 1, ATP series ZLD 5.10 through 5.21 Patch 1, VPN series ZLD 4.60 through 5.21 Patch 1	OS command injection
CVE-2022-26134	Atlassian	Confluence Data Center	7.18.0	OGNL Injection
		Confluence server		
CVE-2022-20707	Cisco	Small Business Series Routers	RV160, RV260, RV340, and RV345	RCE

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2022-1388	F5	BIG-IP	16.1.x versions prior to 16.1.2.2, 15.1.x versions prior to 15.1.5.1, 14.1.x versions prior to 14.1.4.6, 13.1.x versions prior to 13.1.5, all 12.1.x and 11.6.x versions	Authentication bypass
CVE-2021-46422	Telesquare	SDT-CW3B1	1.1.0	OS command injection
CVE-2021-45511	NETGEAR	NETGEAR	AC2100 before 2021-08-27, AC2400 before 2021-08-27, AC2600 before 2021-08-27, D7000 before 2021-08-27, R6220 before 2021-08-27, R6230 before 2021-08-27, R6260 before 2021-08-27, R6330 before 2021-08-27, R6350 before 2021-08-27, R6700v2 before 2021-08-27, R6800 before 2021-08-27, R6850 before 2021-08-27, R6900v2 before 2021-08-27, R7200 before 2021-08-27, R7350 before 2021-08-27, R7400 before 2021-08-27, R7450 before 2021-08-27	Authentication bypass
CVE-2021-44228	Apache	Log4j2	2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1)	Input validation code execution
CVE-2021-36260	Hikvision	Web servers firmware	Various DS-2CD, DS-2X, DS-2DY, PTZ-N, DS-2DF, DS-2TD, IDS, DS-76, DS-71	Command injection

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2021-28799	QNAP Systems Inc.	Hybrid Backup Sync (HBS) 3	versions prior to v16.0.0415 on QTS 4.5.2; versions prior to v3.0.210412 on QTS 4.3.6; versions prior to v3.0.210411 on QTS 4.3.4; versions prior to v3.0.210411 on QTS 4.3.3; versions prior to v16.0.0419 on QuTS hero h4.5.1; versions prior to v16.0.0419 on QuTScloud c4.5.1~c4.5.4	Improper authorization
CVE-2021-20090	Buffalo Arcadyan	Buffalo WSR Arcadyan firmware	WSR-2533DHPL2 firmware version <= 1.02, WSR-2533DHP3 firmware version <= 1.24	Path traversal
CVE-2021-1473	Cisco	Small Business RV Series Routers	RV340/RV340W, RV345/RV345P before 1.0.03.21	OS command injection
CVE-2021-1472	Cisco	Small Business Series Routers firmware	RV160, RV160W, RV260, RV260P, RV260W, RV340, RV340W, RV345, RV345P	Arbitrary code execution
CVE-2020-8515	DrayTek	Vigor	Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, 1.4.4_Beta	RCE
CVE-2020-4450	IBM	WebSphere Application Server	8.5 and 9.0 traditional	Arbitrary code execution
CVE-2020-35391	Tenda	Tenda F3 Firmware	Tenda F3 Firmware 12.01.01.48	Forced browsing

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2020-3452	Cisco	Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) Software	ASA <9.6.4.42, <9.8.4.20, <9.9.2.74, <9.10.1.42, <9.12.3.12, <9.13.1.10, <9.14.1.10 FTD <6.2.3.16, <6.3.0.6, <6.4.0.10, <6.5.05, <6.6.0.1	Path traversal
CVE-2020-3451	Cisco	Small Business Series Routers Firmware	RV340W, RV340, RV345, RV345P	Multiple Security Vulnerabilities – like Buffer overflow via environment variables, server side include (SSI) injection
CVE-2020-15415	DrayTek	Vigor Firmware	3900, 2960, and 300b	Command injection
CVE-2019-7256	Linear eMerge	E3-Series	Nortekcontrol Linear Emerge Essential Firmware Nortekcontrol Linear Emerge Elite Firmware	Command injection
CVE-2019-19824	TOTOLINK Realtek	SDK based routers	A3002Ru through 2.0.0, A702R through 2.1.3, N301Rt through 2.16, N302R through 3.4.0, N300Rt through 3.4.0, N200Re through 4.0.0, N150Rt through 3.4.0, N100Re through 3.4.0, N302RE through 2.0.2	OS command injection

CVE	Vendor	Product	Versions affected	Vulnerability type
CVE-2019-17621	D-Link	DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01	DIR-818Lx Bx <=v2.05b03_Beta08, DIR-822 Bx <=v2.03b01, DIR-822 Cx <=v3.12b04, DIR-823 Ax <=v1.00b06_Beta, DIR-859 Ax <=v1.06b01Beta01, DIR-868L Ax <=v1.12b04, DIR-868L Bx <=v2.05b02, DIR-869 Ax <=v1.03b02Beta02, DIR-880L Ax <=v1.08b04, DIR-890L/R Ax <=v1.11b01_Beta01, DIR-885L/R Ax <=v1.12b05, DIR-895L/R Ax <=v1.12b10	OS command injection related to UPnP service
CVE-2019-12168	Four-Faith	Four-Faith Wireless Mobile Router F3x24	Firmware 1.0	RCE via command shell
CVE-2019-11829	Microsoft	Windows 10 Server 2016	Server 2016 1607 1703	OS command injection
CVE-2018-18852	Cerio	Cerio Dt-300N Firmware Cerio Dt-300n	DT-300N 1.1.6 through 1.1.12 devices	OS command injection
CVE-2017-7876	QNAP	QTS	QTS 4.2.6 before build 20170517, QTS 4.3.3.0174 before build 20170503	Command injection
CVE-2015-7450	IBM	Tivoli Common Reporting	3.1.0.2, 3.1, 3.1.2, 3.1.2.1, 2.1, 2.1.1.2, 3.1.0.1, 2.1.1,	Code injection