ZERO DAY VULNERALABILTIES

[1]VaibhavSingh, [2]Bhawna Kaushik, [3]Priya Gupta , [4]Anam Shariq

1.niu-23-11977@niu.edu.in

2. bhawna.kaushik@niu.edu.in

3. priya.gupta@niu.edu.in

[1,2,3]NoidaInternationalUniversity,Sector17A,GreaterNoida, [4]Birla Public School Qatar

Abstract

This paper explores the growing threat of zero-day exploits and their profound impact on national infrastructure and security. Zero-day vulnerabilities, undiscovered by software vendors, allow attackers to exploit critical systems without immediate detection. By examining real-world examples suchasStuxnetandWannaCry,theresearchhighlightshowtheseexploitstargetgovernment,military, and essential services. The paper also discusses current detection methods, mitigation strategies, and the role ofAI in identifying emerging vulnerabilities. With Cyber threats evolving, the study emphasizes theneedfor proactivesecuritymeasurestosafeguardnationalinterestsagainstthis hidden danger.

Keywords:Zero-Dayvulnerabilities,StuxnetandWannaCry,CyberThreats

UnderstandingZero-DayExploits

Azeroday(or 0-day) vulnerabilityis a securityriskina piece of softwarethat is not publicly known about andthevendor is not awareof.Azero- day exploit is the methodanattacker uses toaccess the vulnerablesystem.Theseareseveresecuritythreats withhighsuccess ratesas businesses donot have defenses in place to detect or prevent them.

Azerodayattackis so-calledbecauseit occurs beforethetarget is awarethat thevulnerability exists. The attacker releases malware before the developer or vendor has had the opportunity to create a patch to fix the vulnerability.

Azero-dayattackbegins witha hacker discoveringa zero-dayvulnerability, which is an error incode or softwarethatthetargethasyettodiscover.Theattacker thenworksona zero-dayexploit, a method of attack, that they can use to take advantage of the existing vulnerability.

Top10RoutinelyExploitedVulnerabilitiesin2023(ConsideredAsAZero-Day)

ExploitedCVEsof2023Are:

1. CVE-2023-3519:CriticalVulnerability,allowsanunauthenticateduser tousea HTTPGET request to cause a stack buffer overflow in the NetScaler Packet Processing Engine (nsppe). Attackers can leverage this exploit to upload malicious files that enable remote control execution, privilege escalation, and credential access.

2. CVE-2023-4966:CriticalVulnerability,allowsattackerstoreadmemoryoutsidebuffers, including session tokens (session token leakage), allowing attackers to impersonate authenticated users. Once the attacker has exploited this vulnerability, they can use it to perform reconnaissance on hosts and networks, harvest credentials .

3. CVE-2023-20198 : The attacker first exploited CVE-2023-20198 to gain initial access and issueda privilege15commandtocreatea localuser andpasswordcombination.Thisallowed theuser to log in with normal user access. Theattacker then exploited another component of the web UI feature, leveraging the new local user to elevate privilege to root and write the implant to the file system.

4. CVE-2023-20273:HighRisk,TargetsCiscoIOSXE,buildinguponCVE-2023-20198.It leverages CVE-2023-20198 by using command injections to escalate privileges to root privileges.

5. CVE-2023-27997:It’sa heap-basedbuffer overflowinFortiGate'sSSLVPNcomponent which has been demonstrated to be exploitable for pre-authentication RCE. Since this a memory corruption bug, we to be able to detect vulnerable versions without crashing thesslvpndprocess anddisconnectingactiveusers.

6. CVE-2023-34362 : CVE-2023-34362 is a significant vulnerability that could potentially enableanunauthenticatedattacker toaccess andmanipulatea business'sdatabasethrougha method known as SQL injection. If left unaddressed, this vulnerability could lead to significant data breaches, loss of sensitive information, and severe disruption of services.

   ThevulnerabilityarisesfromaninsecureSQLqueryin
   the UserEngine.UserGetUsersWithEmailAddress() function (defined in MOVEit.DMZ.ClassLib), whichisbuiltbyconcatenatingstringssuppliedasparametersto the function .

   CVE-2023-22515 : Severity Critical (9.8) -Atlassian Confluence is affected by this CVE an AuthenticationBypass vulnerability.Theroot causeof this vulnerabilityistheexistenceofan access path that does not have authentication checks. An attacker can access the /server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false path, which requiresnoauthentication, toset theapplicationinSetupMode. Inthis mode, theattacker can create an admin user with no authentication requirements. Using this newly created user the attacker has full access to the web interface of theAtlassian Confluence target.

7. CVE-2021-44228 :Aremote code execution (RCE) Vulnerability inApache Log4j2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform. By submittinga speciallycraftedrequest toa vulnerablesystem, depending onhowthesystemis configured, anattacker is abletoinstruct thatsystemto downloadandsubsequentlyexecutea malicious payload. Due to the discovery of this exploit being so recent, there are still many servers, both on-premises and within cloud environments, that have yet to be patched. Like many high severity RCE exploits, thus far, massive scanning activity for CVE-2021-44228 hasbegunontheinternetwiththeintentofseekingoutandexploitingunpatchedsystems.We

highlyrecommendthat organizations upgradetothelatest version(2.17.1) ofApacheLog4j2 for all systems. This version also patches the additional vulnerabilities CVE-2021-45046, foundonDec. 14; CVE-2021-45105, foundonDec. 17;andCVE-2021-44832, foundonDec. 28

8. CVE-2023-2868 : This Vulnerability , targets the Barracuda Networks Email Security Gateway(ESG)Appliance. It allows badactorstoleverageinput validationandsanitization errorstoobtainunauthorizedaccessandremotelyexecutesystemcommands.ThisisUnder Critical Vulnerability

9. CVE-2022-47966 :This Vulnerability allow remote code execution due to use of ApacheSantuario xmlsec (aka XMLSecurity for Java) 1.4.1, because the xmlsec XSLT features, bydesign in that version, make the application responsible for certain security protections, andthe ManageEngine applications did not provide those protections. This affects Access Manager Plus before 4308,Active Directory 360 before 4310,ADAudit Plus before 7081, ADManager Plus before7162,ADSelfServicePlus before6211,Analytics Plus before5150, ApplicationControlPlus before10.1.2220.18,Asset Explorer before6983, Browser Security Plus before 11.1.2238.6, Device Control Plus before 10.1.2220.18, Endpoint Central before 10.1.2228.11,EndpointCentralMSPbefore10.1.2228.11,EndpointDLPbefore10.1.2137.6, Key Manager Plus before 6401, OS Deployer before 1.1.2243.1, PAM 360 before 5713, Password Manager Pro before 12124, Patch Manager Plus before 10.1.2220.18, Remote Access Plus before 10.1.2228.11, Remote Monitoring and Management (RMM) before 10.1.41.ServiceDeskPlusbefore14004,ServiceDeskPlusMSPbefore13001,SupportCenter Plus before 11026, and Vulnerability Manager Plus before 10.1.2220.18.

Real-WorldCaseStudies

- **Maliciouscampaigns,whichleveragedzero-day vulnerabilities.**
- **Tablebelowcontainsdescriptionofallmajorincidentsoccurredwithinthelast 11 years between 2006 and 2016.**

Name	Description	Vulnerability
AdGholas	The attacks were active since at least October 2015.Toavoiddetection the hackers use steganography and file whitelistingtechniques.	CVE-2016-3351 CVE-2016-3298 CVE-2017-0022
Amnesty International HongKongsitebreach	Thehackerscompromised the website and were deliveringTrojanGh0st RAT.	CVE-2010-2884 CVE-2012-1889
IceDaggerattack	Theattackiscalled“Ice Dagger” by Adallom securityfirmduetoits sophistication.	CVE-2013-5054

Luckycat attacks	The campaign has been active since at least June 2011 and linked to 90 attacksagainstIndianand Japan institution.	CVE-2010-3654
OperationRussianDoll	The operation refers to the Russian Hacker group APT28. The hackers are suspectedtotargetGerman parliament, French television network TV5Monde, the White House, andNATO.	CVE-2015-1701

TheRealStoryOfStuxnet

Computer cables snake across the floor. Cryptic flowcharts are scrawled across various whiteboards adorningthewalls.Alife-sizeBatmandollstandsinthehall.Thisofficemight seemnodifferent than any other geeky workplace, but in fact it’s the front line of a war—a cyberwar, where most battles play out not in remote jungles or deserts but in suburban office parks like this one.

Recognition of such threats exploded in June 2010 with the discovery of Stuxnet, a 500-kilobyte computer worm that infected the software of at least 14 industrial sites including a uranium-enrichment plant. Althougha computer virus relies on anunwitting victim oinstallit, a worm spreads on its own, often over a computer network.

AboutThisWorm:StuxnetcouldspreadstealthilybetweencomputersrunningWindows—eventhose not connected to the Internet. If a worker stuck a USB thumb driveinto an infected machine, Stuxnet could, well, worm its way onto it, then spread onto the next machine that read that USB drive. Because some one could unsuspectingly infecta machine this way, letting the wormproliferateover local area networks, experts feared that the malware had perhaps gone wild across the world.

Illustration:L-Dopa

InOctober 2012,U.S.defensesecretaryLeonPanetta warnedthat theUnitedStateswasvulnerableto a “cyber Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The next month, Chevron confirmed the speculation by becoming the first U.S. corporation to admit that Stuxnet had spread across its machines.

ThePotentialDamageofWannaCryRansomwareAttack

- Thewidespreadofthe mal ware,andthedamage it caused, meant thatthethree-day attack carried an estimated global cost in the billions.

- However, the damage caused by Wannacry was not evenly spread across different businesses and industries. Organizations like the UK’s National Health Service (NHS),whichwasrunninga largenumberofvulnerable machines,wereespecially hard hit.The cost ofWannacrytothe NHS alone is estimatedtobeUS $100 Million.

- The 2017 outbreak was only stopped by the discovery of a “kill switch” within the WannaCrycode,which,whentriggered,stoppedthemalwarefromspreadingfurther or encrypting the data stored on any additional machines. Since the 2017 outbreak, additionalattacksbymodified versionsofWannaCryhaveoccurred. However, none of them have achieved the same footprint, cost, or recognition as the original outbreak.

HowWannaCryWorks?

1. Infection:Unlikemanyotherransomwarevariants,WannaCryspreadsonitsownratherthan being carried by malicious emails or installed via malware droppers.

WannaCry’swormfunctionalitycomesfromitsuseoftheEternalBlueexploit,whichtakes advantage of a vulnerability in Windows ‘Server Message Block (SMB) protocol. The vulnerability was first discovered by the National Security Agency (NSA) and publicly leaked by the Shadow Brokers.

Machines infected withWannaCryscanthe Internet for other machines running a vulnerable version ofSMB. If one is found, the infected computer uses Eternal Blue to send and run a copy of WannaCryon the targeted computer. At this point, the malware could begin encryption of the computer’s files. However, first it checks for the existence ofa particular website. If the website exists, then the malware does nothing. The presence of this “kill switch” is theorized to be either a way to stop the spread ofWannaCry(which spreads independently once launched)orasameansofmaking forensicanalysismoredifficult (since most cybersecurity lab environments will pretend that any website that the malware requests exists). If the requested domain is not found, WannaCryproceeds to the encryption stage.

2. Encryption

WannaCry is designed to deny a user access to their files on a computer unless a ransom is paid.Thisisaccomplishedthroughtheuseofencryption,wherethe malwaretransformsthe data in a waythat is onlyreversible with knowledge of the secret key. Since WannaCry’s secret keyisonlyknownto the ransom ware operator, this forces a victims pay the ransom to retrieve their data.

Winery is designed to search for and encrypt a set list office extension types on a computer.Thisisdonetominimizethe malware’simpact onasystem’sstability.Acomputer maynot beabletorunifthewrongfilesareencrypted,making it impossible forthevictimto pay a ransom or retrieve their files.

3. Ransom

The WannaCry malware demanded a ransom of US$300 from its victims. However, the ransomdemand was to pay in Bitcoin, not fiat money.As a cryptocurrency, Bitcoin is less traceablethantraditionaltypesofcurrency,whichishelpfulforransomwareoperatorssince it allowsthemtoembedapayment address(similarto abankaccount number) inaransom message without it immediately alerting the authorities to their identity.

Ifa victimofa WannaCryattack paysthe ransom, theyshould be provided witha decryption key for their computer.This enables a decryption programprovided by the cybercriminals to reversethetransformationperformedontheuser’sfilesand returnaccesstotheoriginaldata.

ImpactonNationalSecurity

Zero-day attacks, which exploit previously unknown vulnerabilities, pose significant threats tonationalsecurity.Theseattackscancompromisesensitivegovernment data,disrupt critical infrastructure, and undermine public trust. Here are some notable instances and analyses highlighting their impact:

StuxnetWorm(2010)

Stuxnet isaprimeexampleofazero-dayattackwithprofoundnationalsecurityimplications. Discovered in 2010, this sophisticated worm exploited multiple zero-day vulnerabilities to target Iran's nuclear enrichment facilities, causing significant disruptions. The attack underscored the potential ofzero-dayexploits in cyber warfare, demonstrating how theycan be used to achieve strategic objectives without traditional military engagement.

ShadowBrokersLeak(2016)

In 2016, a group knownas the Shadow Brokersreleased a cache ofsophisticated zero-day exploitsallegedlystolenfromtheU.S.NationalSecurityAgency(NSA).Amongthesewas "EternalBlue," which was later used in widespread attacks like WannaCry and NotPetya, causing global disruptions. This incident highlighted the risks associated with stockpiling zero-day vulnerabilities, as their exposure can lead to widespread exploitation.

ChineseCyberEspionageActivities

Chinesestate-sponsoredhackinggroupshavebeenimplicated innumerouscyberespionage campaigns targeting various countries' critical infrastructure. For instance, inApril 2021, suspected Chinese hackers exploited a zero-day vulnerability in Pulse Connect Secure devices to spyon government and defense industrytargets in the U.S. and Europe. Such activities underscore the persistent threat posed by zero-day exploits in international cyber espionage.

Identify,Protect,Detect,Respond,Recover–NationalSecurtiyAgency|UnitedStatesOfAmerica

DetectionandMitigationStrategies

- **NSA'STop10CybersecurityMitigationStrategies:**

1. **UpdateandUpgradeSoftwareImmediately**
2. **DefendPrivilegesandAccounts**
3. **EnforceSignedSoftwareExecutionPolicies**
4. **ExerciseaSystemRecoveryPlan**
5. **ActivelyManageSystemsandConfigurations**
6. **ContinuouslyHuntforNetworkIntrusions**
7. **LeverageModernHardwareSecurityFeatures**
8. **SegregateNetworksUsingApplication-AwareDefenses**
9. **IntegrateThreatReputationServices**
10. **TransitiontoMulti-FactorAuthentication**

FutureTrendsandChallenges

Remoteworkingcybersecurityrisks:TheCovid-19pandemic forcedmostorganizationsto shift their workforces to remote work, often quite rapidly.

Working from home poses new cybersecurityrisks and is one of the most talked-about new trendsincybersecurity.Homeofficesareoftenlessprotectedthancentralizedoffices,which tendto have moresecure firewalls, routers,and access management runbyITsecurityteams. In the rush to keep things operational, traditional securityvetting may not have been as rigorous as usual – with cybercriminals adapting their tactics to take advantage.

The Internet ofThings (IoT) evolving : The expanding Internet ofThings (IoT) creates moreopportunitiesforcybercrime.TheInternetofThingsreferstophysicaldevicesother than computers, phones, and servers, which connect to the internet and share data.

Itisestimatedthatby2026, therewillbe64billionIoTdevices installedaroundtheworld. The trend towards remote working is helping to drive this increase.

IoT devices have fewer processing and storage capabilities. This can make it harder to employfirewalls,antivirus,andothersecurityapplicationstosafeguardthem.Asaresult,IoT attacks are amongst the discussed cyber-attack trends

The rise of ransom ware :Ransomwareisn'ta newthreat –it'sbeenaroundfor abouttwodecades – but it is a growing one. It's estimated that therearenowover 120 separatefamilies of ransomware, and hackers have become very adept at hiding malicious code. Ransomware is a relatively easy way for hackers togainfinancialrewards, which is partlybehind its rise.Another factor was theCovid-19 pandemic. Theaccelerated digitization of many organizations, coupled with remote working, created newtargetsfor ransomware. Boththevolumeofattacksandthesize of demandsincreasedasaresult.

Extortion attacks involve criminals stealing a company's data and then encrypting it so they can't access it.Afterward, cybercriminals blackmail the organization, threatening to release itsprivatedataunlessaransomispaid.Theburdenofthiscyberthreat issignificant giventhe sensitive data at stake as well as the economic impact of paying the ransom.

Increasein cloud servicesand cloud security threats: Cloud vulnerabilitycontinuesto be oneofthebiggest cybersecurityindustrytrends.Again, therapidandwidespreadadoptionof remoteworking following the pandemic increased the necessityfor cloud-based services and infrastructure .

Cloudservicesoffer arangeofbenefits –scalability, efficiency, andcostsavings. Butthey arealso aprimetarget forattackers.Misconfiguredcloudsettingsareasignificant causeof data breaches and unauthorized access, insecure interfaces, and account hijacking. The average cost of a data breach is $3.86 million.

Socialengineeringattacks:SocialEnginneringattackslikephishingarenotnewthreatsbut have become more troubling amid the widespread remote workforce.Attackers target individuals connecting to their employer's network from home because they make easier targets.As well as traditional phishing attacks on employees, there has also been an uptick inwhalingattackstargetingexecutiveorganizationalleadership.

SMSphishing–sometimesknownas'smishing'–isalso gainingprominence, thankstothe popularityofmessagingappssuchasWhatsApp,Slack,Skype,Signal,WeChat,andothers. Attackers use these platforms to tryto trick users into downloading malware onto their phones.

Voicephishing–alsocalled'vishing'–whichgainedprominenceinaTwitterhackin2020. Hackers posing as IT staff called customer service representatives and tricked them into providing access to an important internaltool. Vishing has been used to target numerous companies, including financial institutions and large corporates.

SIM jacking, where fraudsters contact the representatives of the mobile operator of a particularclient andconvincethemthattheirSIMcardishacked.Thismakesit necessaryto transfer the phone number to another card. If the deception is successful, the cybercriminal gains access to the digital contents of the target's phone.

Organizationsareincreasingtheirprotectionagainstphishing,butcriminalsarealways looking for new ways to stay ahead.

Conclusion

Zero-dayattacks, exploitingunknownsoftwarevulnerabilities, posea significantthreattonational security. Their unpredictable nature makes them particularly dangerous, as organizations cannot prepare for unknown threats, allowing attackers to bypass existing security measures.

The2010Stuxnetwormexemplifiesthisdanger, wheremultiplezero-dayexploitswereusedtotarget Iran's nuclear facilities, causing significant disruptions.

Similarly, in2021, suspectedChinesehackersutilizeda zero-dayattackagainstPulseConnectSecure devices to spy on government and defense industry targets in the U.S. and Europe.

These incidents highlight the critical need for robust cybersecurity measures and international cooperationtomitigatetherisksassociatedwithzero-dayvulnerabilities. Establishingnormsagainst the use of zero-day exploits could enhance global security.

In conclusion, addressing the challenges posed by zero-day attacks is essential for safeguarding nationalsecurity.Proactivestrategies,includingtimelypatchingofvulnerabilitiesandinternational collaboration, are vital to defend against these covert threats.

References

BishopFox.(2023). *CVE-2023-27997-check*. GitHub.

Cobalt.(2023).*2023’sTopRoutinelyExploitedVulnerabilities*. Fortinet.

(n.d.-a). *Exploit.*

Fortinet.(n.d.-b).*Zero-dayattack.*

HackTheBox.(2023).*CVE-2023-34362Explained*. IEEE

Spectrum. (2019). *The real story of Stuxnet*.

Kaspersky. (2023). *Cybersecurity trends.*

ManageEngine.(2023).*CVE-2022-47966Advisory*.

Mitre. (2023). *CVE-2023-20198.*

NationalSecurityAgency.(2023).*NSA’sTop10CybersecurityMitigationStrategies.*

Packet StormSecurity.(2023a).*ZohoManageEngineServiceDeskPlus14003RemoteCode Execution.*

PacketStormSecurity.(2023b). *ManageEngineADSelfServicePlusUnauthenticatedSAML Remote Code Execution*.

Packet StormSecurity.(2023c).*ZohoManageEngineEndpointCentralMSP10.1.2228.10 Remote Code Execution*.

PaloAltoNetworksUnit42.(2021).*ApacheLog4jVulnerabilityCVE-2021-44228*.

Pentest-Tools. (n.d.). *Atlassian Confluence Authentication Bypass*.

Rapid7.(2023).*CVE-2022-47966Analysis*.

U.S.CyberCommand.(2017). *StockpilingZero-DayExploits:TheNextInternational Weapons Taboo?*.

U.S.CybersecurityandInfrastructureSecurityAgency(CISA). (2023). *AA23-250A: Exploited Vulnerabilities*.

ViettelCyberSecurity.(2023).*SAMLShowStopper*.

Wikipedia. (n.d.-a). *Cyberwarfare by China*.

Wikipedia.(n.d.-b).*Zero-dayvulnerability*.

Zero-Day.cz. (n.d.). *Research*.

Horizon3.ai.(2023a).*ManageEngineCVE-2022-47966TechnicalDeepDive*.

Horizon3.ai. (2023b). *CVE-2022-47966 Proof of Concept*. GitHub.

ApacheSantuario.(n.d.). *XMLSecurityforJavaReleases*.GitHub.