FORTINET

OUTBREAK ALERTS

CISA Top 20 Vulnerabilities

Actively exploited CVEs by Chinese State-Sponsored Cyber Actors since 2020

https://www.cisa.gov/uscert/ncas/alerts/aa22-279a
CVEs: CVE-2021-44228, CVE-2019-11510, CVE-2021-22205, CVE-2021-22005, CVE-2019-19781, CVE-2021-1497, CVE-2021-20090, CVE-2021-42237, CVE-2022-24112, CVE-2022-26134, CVE-2021-26855, CVE-2020-5902, CVE-2021-26084, CVE-2021-36260, CVE-2022-1388, CVE-2021-40539, CVE-2021-20857, CVE-2021-26858, CVE-2021-27065, CVE-2021-41773

Joint Cybersecurity Advisory (CSA) has released the top Common Vulnerabilities and Exposures (CVEs) used since 2020 by Peoples Republic of China (PRC) state-sponsored cyber actors as assessed by the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI).

Previously, FortiGuard labs has already published various Outbreaks Alerts included in the released CISA's advisory such as: Apache Log4j, Hikvision Webserver Vulnerability, Atlassian Confluence OGNL RCE Vulnerability, Microsoft Exchange Server RCE Vulnerabilities etc. See the full list at: https://www.fortiguard.com/outbreak-alert

Links to dedicated reports on each published outbreak by FortiGuard Labs are added to Additional Resources section below.

Background

The list below shows the FortiGuard IPS signature protections against published CISA top 20 Vulnerabilities:
1. Apache.Log4j.Error.Log.Remote.Code.Execution
2. Pulse.Secure.SSL.VPN.HTML5.Information.Disclosure
3. GitLab.Community.and.Enterprise.Edition.Command.Injection
4. Atlassian.Confluence.OGNL.Remote.Code.Execution
5. MS.Exchange.Server.PrivateRegistryHandler.Remote.Code.Exec
6. F5.BIG-IP.Traffic.Management.User.Interface.Directory.Traversal
7. VMware.vCenter.Server.Analytics.Arbitrary.File.Upload
8. Citrix.Application.Delivery.Controller.VPNs.Directory.Traversal
9. Cisco.HyperFlex.HX.Auth.Handling.Command.Injection
10. Arcadyan.Routers.images.Path.Authentication.Bypass
11. Atlassian.Confluence.CVE-2021-26084.Remote.Code.Execution
12. Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection
13. Sitecore.XP.Insecure.Deserialization.Remote.Code.Execution
14. F5.BIG-IP.Control.REST.Authentication.Bypass
15. APSISX.Admin.API.default.token.Remote.Code.Execution
16. Zoho.ManageEngine.ADSelfService.Plus.Authentication.Bypass
17. MS.Exchange.Server.UM.Core.Remote.Code.Execution
18. MS.Exchange.Server.CVE-2021-26858.Remote.Code.Execution
19. MS.Exchange.Server.CVE-2021-27065.Remote.Code.Execution
20. Apache.HTTP.Server.cgi.bin.Path.Traversal

Announced

October 06, 2022: CISA released the advisory:
https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

In the published advisory, NSA, CISA, and FBI has urged U.S. and allied governments, critical infrastructure, and private sector organizations to apply mitigations, increase their defensive posture and reduce the threat of compromise from PRC state-sponsored malicious cyber actors.

Latest Developments

October 18, 2022: FortiGuard Labs Researchers are continually working on protecting organizations and releasing automated signature updates throughout the Security Fabric such as:

Next-Gen Intrusion preventions systems (IPS):
https://www.fortinet.com/products/next-generation-firewall
FortiClient Endpoint Security Fabric Agent:
https://www.fortinet.com/products/endpoint-security/forticlient
FortiWEB Web Application Firewall (WAF):
https://www.fortinet.com/products/web-application-firewall/fortiweb

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery

Vulnerability

Detects and Blocks attack attempts related to CISA Top 20 Vulnerabilities

FortiClient
DB 1.348

- Exploitation

IPS

Detects and Blocks attack attempts related to CISA Top 20 Vulnerabilities

FortiGate *DB 22.414* | FortiSASE *DB 22.414* | FortiNDR *DB 22.414* | FortiADC *DB 22.414* | FortiProxy *DB 22.414*

Web App Security

Detects and Blocks attack attempts related to CISA Top 20 Vulnerabilities

FortiWeb *DB 0.00330* | FortiADC *DB 1.00038*

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient *DB 1.003* | FortiAnalyzer *DB 1.00067*

IOC

FortiAnalyzer *DB 0.02355* | FortiSIEM *DB 0.02355* | FortiSOCaaS *DB 0.02355*

Threat Hunting

FortiAnalyzer *v7.0+* | FortiSIEM *v6.6.0*

Content Update

FortiSIEM
DB 308

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response | FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

FortiRecon: EASM

Additional Resources

CISA Alert	https://www.cisa.gov/uscert/ncas/alerts/aa22-279a
Fortinet Threat Signal	https://www.fortiguard.com/encyclopedia/ips?id=47196
1. Apache Log4j2	https://www.fortiguard.com/outbreak-alert/log4j2-vulnerability
2. Pulse Connect Secure	https://www.fortiguard.com/encyclopedia/ips/48342
3. GitLab CE/EE	https://www.fortiguard.com/encyclopedia/ips/50901
4. Atlassian Confluence OGNL	https://www.fortiguard.com/outbreak-alert/confluence-ognl
5. Microsoft Exchange Server	https://www.fortiguard.com/outbreak-alert/microsoft-exchange
6. F5 Big-IP	https://www.fortiguard.com/encyclopedia/ips/49330
7. VMware vCenter Server	https://www.fortiguard.com/encyclopedia/ips/50789
8. Citrix ADC	https://www.fortiguard.com/encyclopedia/ips/48653
9. Cisco Hyperflex	https://www.fortiguard.com/encyclopedia/ips/50457
10. Buffalo WSR	https://www.fortiguard.com/encyclopedia/ips/50658
11. Atlassian Confluence	https://www.fortiguard.com/encyclopedia/ips/50727
12. Hikvision IP Cameras	https://www.fortiguard.com/outbreak-alert/hikvision-command-injection
13. Sitecore XP	https://www.fortiguard.com/encyclopedia/ips/50936
14. F5 Big-IP	https://www.fortiguard.com/encyclopedia/ips/51543
15. Apache	https://www.fortiguard.com/encyclopedia/ips/51298
16. Zoho ManageEngine	https://www.fortiguard.com/outbreak-alert/zoho-exploit
17. Microsoft Exchange Server	https://www.fortiguard.com/outbreak-alert/microsoft-exchange
18. Microsoft Exchange Server	https://www.fortiguard.com/encyclopedia/ips/49954
19. Microsoft Exchange Server	https://www.fortiguard.com/encyclopedia/ips/49952
20. Apache HTTP Server	https://www.fortiguard.com/outbreak-alert/apache-path-traversal

Learn more about FortiGuard Outbreak Alerts