

Russian Cyber Espionage Attack

Russia's Cyber Unit Targets Global Infrastructure

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a>

CVEs: CVE-2020-1472, CVE-2021-26084, CVE-2021-3156, CVE-2021-4034, CVE-2022-27666, CVE-2021-33044, CVE-2021-33045, CVE-2022-26134, CVE-2022-26138, CVE-2022-3236

FortiGuard Labs continues to observe attack attempts exploiting the vulnerabilities highlighted in the recent CISA advisory about Russian military cyber actors. These actors are targeting U.S. and global critical infrastructure to conduct espionage, steal data, and compromise or destroy sensitive information.

Background

Unit 29155 cyber actors are known to target critical infrastructure and key resource sectors, including the government services, financial services, transportation systems, energy, and healthcare sectors of NATO members, the EU, Central American, and Asian countries since 2020.

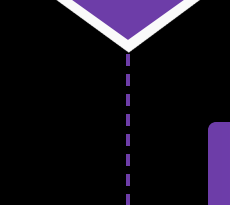
CISA's analysis concluded Unit 29155 cyber actors had exploited multiple CVEs for initial access. These CVEs primarily involve remote code execution, authentication bypass, privilege escalation, and buffer overflow issues affecting products and software such as Dahua IP Cameras, Atlassian Confluence Server and Data Center, and Sophos Firewall Vulnerabilities.

According to the advisory, to date, the FBI has observed more than 14,000 instances of domain scanning across at least 26 NATO members and several additional European Union (EU) countries.

Latest Developments

Fortinet Customers remain protected by the FortiGuard IPS (Intrusion Prevention System) Security Service that can detect and block exploit attempts targeting the vulnerabilities listed in the CISA's advisory and has protections against known malware used in the campaigns. Please see the Solution Tab for full list of available protections.

- December 16, 2024: The Federal Bureau of Investigation (FBI) released this Private Industry Notification (PIN) to highlight HiatusRAT scanning campaigns against Chinese-branded web cameras and DVRs. <https://www.ic3.gov/CSA/2024/241216.pdf>
- September 05, 2024: CISA released a joint advisory as a collective assessment of Unit 29155 cyber operations since 2020. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a>
- August 21, 2024: CISA recently added two new vulnerabilities related to CVE-2021-33044, CVE-2021-33045 (Dahua IP Security Cameras) to their Known Exploited Vulnerabilities Catalog. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- June 14, 2023: FortiGuard Labs released a Threat Signal on the related campaigns. <https://www.fortiguards.com/threat-signal-report/5197/>

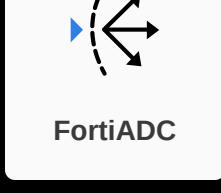


PROTECT

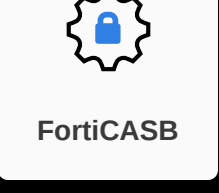
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

AV

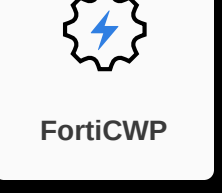
Detects known malware related to the Outbreak



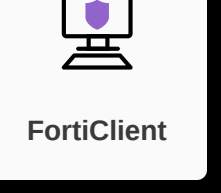
DB 91.02050



DB 91.02050



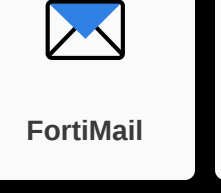
DB 91.02050



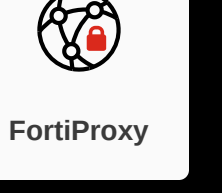
DB 91.02050



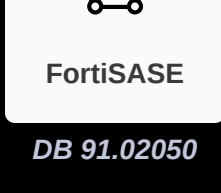
DB 91.02050



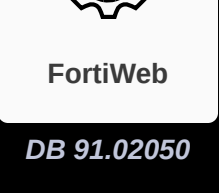
DB 91.02050



DB 91.02050



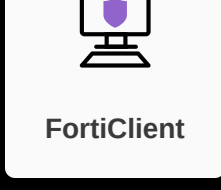
DB 91.02050



DB 91.02050

Vulnerability

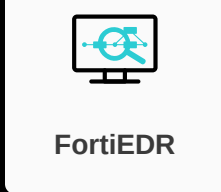
Detects end-user devices running the vulnerable application.



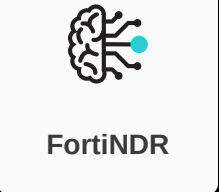
DB 2.355

AV (Pre-filter)

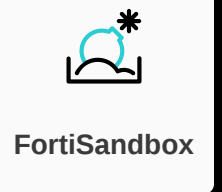
Detects known malware related to the Outbreak



DB 91.02050



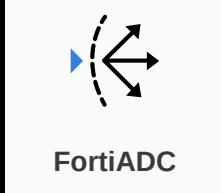
DB 91.02050



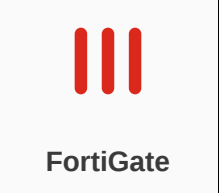
DB 91.02050

IPS

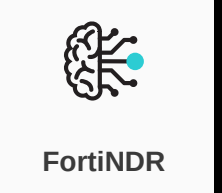
Detects and blocks attack attempts leveraging the vulnerability



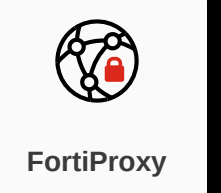
DB 28.859



DB 28.859



DB 28.859



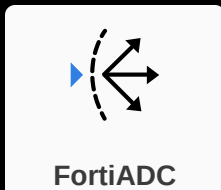
DB 28.859



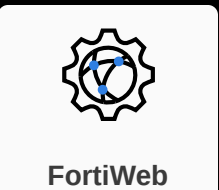
DB 28.859

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

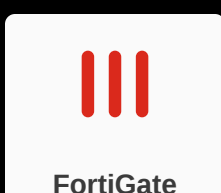


DB 1.00036

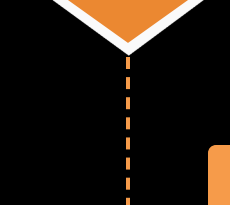


DB 0.00333

IoT/IoT Virtual Patch



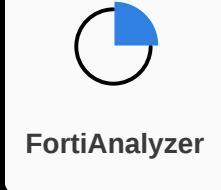
DB 2.355



DETECT

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

IOC



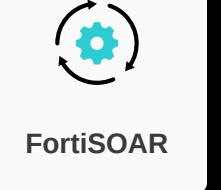
DB 91.02050



DB 91.02050

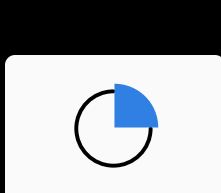


DB 91.02050

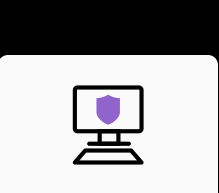


DB 91.02050

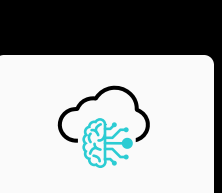
Outbreak Detection



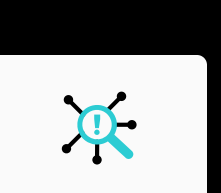
DB 91.02050



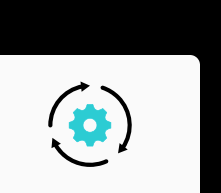
DB 91.02050



DB 91.02050

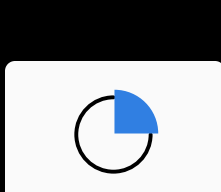


DB 613

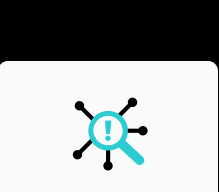


v7.4

Threat Hunting



DB 91.02050



DB 91.02050

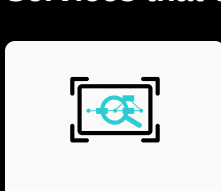


RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

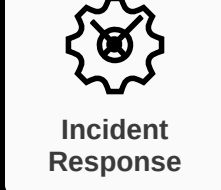
Services that can automatically respond to this outbreak.



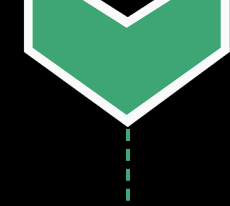
DB 91.02050

Assisted Response Services

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



DB 91.02050

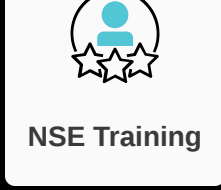


RECOVER

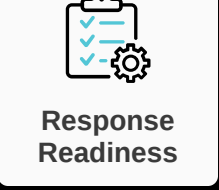
Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



DB 91.02050



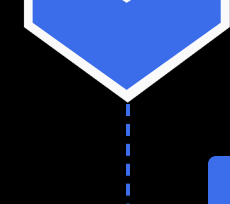
DB 91.02050

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.



DB 91.02050



IDENTIFY

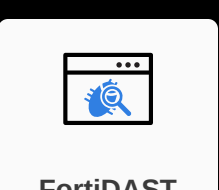
Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



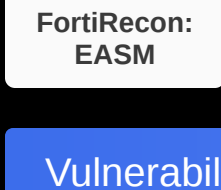
DB 91.02050



DB 91.02050

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.



DB 91.02050

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.



DB 91.02050

Additional Resources

MITRE: WhisperGate <https://attack.mitre.org/software/S0689/>

CISA: Cyber Threat Overview <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia>

CISA: Advisory <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a>

Justice.gov <https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government>

Learn more about [FortiGuard Outbreak Alerts](#)