THREAT ADVISORY

Russian SVR exploits another set of publicly known Vulnerabilities

TA202110

Threat Level Red

Publish Date – May 9, 2021

In accordance with the Threat Advisory released by the Hive Pro threat research team, the Russian SVR aka APT29 continues exploitation of known vulnerabilities to target organizations globally. The threat actors have now expanded their TTPs using multiple publicly available exploit and the Silver framework. The new set of victims include sectors such as governments, think-tank, policy, and energy by deploying an open-source tool Silver which allows the SVR to gain persistence on compromised infrastructure.

The Techniques used by the APT29 includes:

- Active Scanning(T1595.002)
- Exploit PublicFacing Application(T1190)
- Supply Chain Compromise: Compromise Software Supply Chain(T1195.002)
- Trusted Relationship(T1199)
- Command and Scripting Interpreter: Visual Basic(T1059.005)
- Server Software Component: Web Shell(T1505.003)
- Valid Accounts(T1078)

The 7 vulnerabilities targeted are:

- CVE-2019-1653 - Cisco Small Business RV320 and RV325 Routers
- CVE-2019-2725 - Oracle WebLogic Server
- CVE-2019-7609 - Kibana
- CVE-2020-5902 - F5 Big-IP
- CVE-2020-14882 - Oracle WebLogic Server
- CVE-2021-21972 - VMware vSphere
- CVE-2021-26855 - Microsoft Exchange Server

Actor Details

Name	Known as	Origin	Target Locations	Target sectors
APT 29	Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, Grizzly Steppe, CozyCar, CozyDuke	Russia	Austria, Brazil, China, France, Germany, Hungary, Japan, Mexico, Netherlands, New Zealand, Norway, Portugal, South Korea, Spain, Turkey, Ukraine, United States, Uzbekistan	Academic, Aerospace, Energy, Extractive, Financial Services, Government, Industrials, Engineering, Insurance, Media, NGOs, Nonprofits Oil and Gas, Pharmaceuticals, Technology

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2019-1653	Cisco RV320 Dual Gigabit WAN VPN Router version 1.4.2.15 and 1.4.2.17. Cisco RV325 Dual Gigabit WAN VPN Router version 1.4.2.15 and 1.4.2.17.	cpe:2.3:o:cisco:rv320_firmware:1.4.2.15:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv320_firmware:1.4.2.17:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv325_firmware:1.4.2.15:*:*:*:*:*:*:* cpe:2.3:o:cisco:rv325_firmware:1.4.2.17:*:*:*:*:*:*:*	The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information.	CWE-200, CWE-284

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2019-2725	Oracle WebLogic Server versions 10.3.6.0.0 and 12.1.3.0.0.	cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:*	Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	CWE-74
CVE-2019-7609	Kibana versions before 5.6.15 and 6.6.1	cpe:2.3:a:elastic:kibana:*:*:*:*:*:*:*:* cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:*:* cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:*:*	An arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code.	CWE-94
CVE-2020-5902	BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_advanced_firewall_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_advanced_web_application_firewall:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_analytics:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_application_acceleration_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_application_security_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_ddos_hybrid_defender:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_domain_name_system:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_fraud_protection_service:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_global_traffic_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_link_controller:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_local_traffic_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:big-ip_policy_enforcement_manager:*:*:*:*:*:*:*:* cpe:2.3:a:f5:ssl_orchestrator:*:*:*:*:*:*:*:*	The Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	CWE-94
CVE-2020-14882	Oracle WebLogic Server10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0	cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:12.1.3.0.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:12.2.1.3.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:*:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:14.1.1.0.0:*:*:*:*:*:*:*	Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.	
CVE-2021-21972	VMware vCenter Server 7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n and VMware Cloud Foundation 4.x before 4.2 and 3.x before 3.10.1.2	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:6.7:-:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:7.0:-:*:*:*:*:*:*	The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server.	CWE-269

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Description	CWE ID
CVE-2021-26855	Microsoft Exchange Server 2013 CU23/2016 CU18/2016 CU19/2019 CU7/2019 CU8	cpe:2.3:a:microsoft:exchange_server:2013:-:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2016:-:*:*:*:*:*:* cpe:2.3:a:microsoft:exchange_server:2019:-:*:*:*:*:*:*	Microsoft Exchange Server Remote Code Execution Vulnerability	

Patch Links

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-info
http://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html
https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077
https://support.f5.com/csp/article/K52145254
https://www.oracle.com/security-alerts/cpuoct2020.html
https://www.vmware.com/security/advisories/VMSA-2021-0002.html
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855

References

https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf
https://thehackernews.com/2021/05/top-11-security-flaws-russian-spy.html
https://nvd.nist.gov/vuln/detail/CVE-2021-26855
https://nvd.nist.gov/vuln/detail/CVE-2020-14882
https://nvd.nist.gov/vuln/detail/CVE-2020-5902
https://nvd.nist.gov/vuln/detail/CVE-2019-7609
https://nvd.nist.gov/vuln/detail/CVE-2019-2725
https://nvd.nist.gov/vuln/detail/CVE-2019-1653
https://nvd.nist.gov/vuln/detail/CVE-2021-21972