Several Vulnerabilities Found in GE Power Meter Software

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/YkTgiaNfsEg/several-vulnerabilities-found-ge-power-meter-software

---

Google Announces Fourth-Annual Capture the Flag Event

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/2ulPV8IE0H4/google-announces-fourth-annual-capture-flag-event

---

Vulnerabilities Found in Over 100 Jenkins Plugins

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/1_AG-VXdfUg/vulnerabilities-found-over-100-jenkins-plugins

---

DoS Attack Blamed for U.S. Grid Disruptions: Report

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/GyatLK2ERpM/dos-attack-blamed-us-grid-disruptions-report

---

Dell Patches Remote Code Execution Vulnerability in SupportAssist Client

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tUD_6Tfaspo/dell-patches-remote-code-execution-vulnerability-supportassist-client

---

PoC Exploits for Old SAP Configuration Flaws Increase Risk of Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/z9vlWefrtsI/poc-exploits-old-sap-configuration-flaws-increase-risk-attacks

Cisco Patches Critical Vulnerability in Data Center Switches

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/nSNIa1qNrQk/cisco-patches-critical-vulnerability-data-center-switches

---

Many Vulnerabilities Found in Wireless Presentation Devices

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/IlOhYXWJAK4/many-vulnerabilities-found-wireless-presentation-devices

---

Two Vulnerabilities Expose Rockwell Controllers to DoS Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/sBvMgNi

DJUg/two-vulnerabilities-expose-rockwell-controllers-dos-attacks

---

Zero-day attackers deliver a double dose of ransomware—no clicking required

reader comments

56 with 41 posters participating

Share this story

Attackers have been actively exploiting a critical zero-day vulnerability in the widely used Oracle WebLogic server to install ransomware, with no clicking or other interaction necessary on the part of end users, researchers from Cisco Talos said on Tuesday.

The vulnerability and working exploit code first became public two weeks ago on the Chinese National Vulnerability Database, according to researchers from the security educational group SANS ISC, who warned that the vulnerability was under active attack. The vulnerability is easy to exploit and gives attackers the ability to execute code of their choice on cloud servers. Because of their power, bandwidth, and use in high-security cloud environments, these servers are considered high-value targets. The disclosure prompted Oracle to release an emergency patch on Friday.

On Tuesday, researchers with Cisco Talos said CVE-2019-2725, as the vulnerability has been indexed, has been under active exploit since at least April 21. Starting last Thursday—a day before Oracle patched the zero-day vulnerability, attackers started using the exploits in a campaign to install "Sodinokibi," a new piece of ransomware. In addition to encrypting valuable data on infected computers, the malicious program attempts to destroy shadow copy backups to prevent targets from simply restoring the lost data. Oddly enough, about eight hours after infection, the attackers exploited the same vulnerability to install a different piece of ransomware known as GandCrab.

No interaction required

"Historically, most varieties of ransomware have required some form of user interaction, such as a user opening an attachment to an email message, clicking on a malicious link, or running a piece of malware on the device," Talos researchers Pierre Cadieux, Colin Grady, Jaeson Schultz, and Matt Valites wrote in Tuesday's post. "In this case, the attackers simply leveraged the Oracle WebLogic vulnerability, causing the affected server to download a copy of the ransomware from attacker-controlled IP addresses 188.166.74[.]218 and 45.55.211[.]79."

The vulnerability is easy to exploit because all that's required is HTTP access to a vulnerable WebLogic server. Its severity rating under the Common Vulnerability Scoring System is 9.8 out of a possible 10. The attackers send vulnerable servers a POST command that contains a PowerShell command that downloads and then executes a malicious file called "radm.exe." Besides PowerShell, attackers also exploit CVE-2019-2725 to use the Certutil command-line utility. Other files that get downloaded and executed include office.exe and untitled.exe.

The ransom note shown in part above and in full below demands targets pay $2,500 worth of bitcoin within two days to obtain the decryption key that will unlock the encrypted data. After that deadline, the ransom doubles to $5,000. The attackers provide instructions explaining how cryptocurrency novices can establish a bitcoin wallet and obtain the digital currency, going as far as recommending use of Blockchain.info.

Cisco Talos

The attacks are notable for their use of a high-severity zero-day in software that’s widely used in cloud environments. The combination means attacks are likely to continue. Organizations that use WebLogic should make installing

Friday’s patch a top priority.

https://arstechnica.com/?p=1498281