Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:119 **11-12-2020**

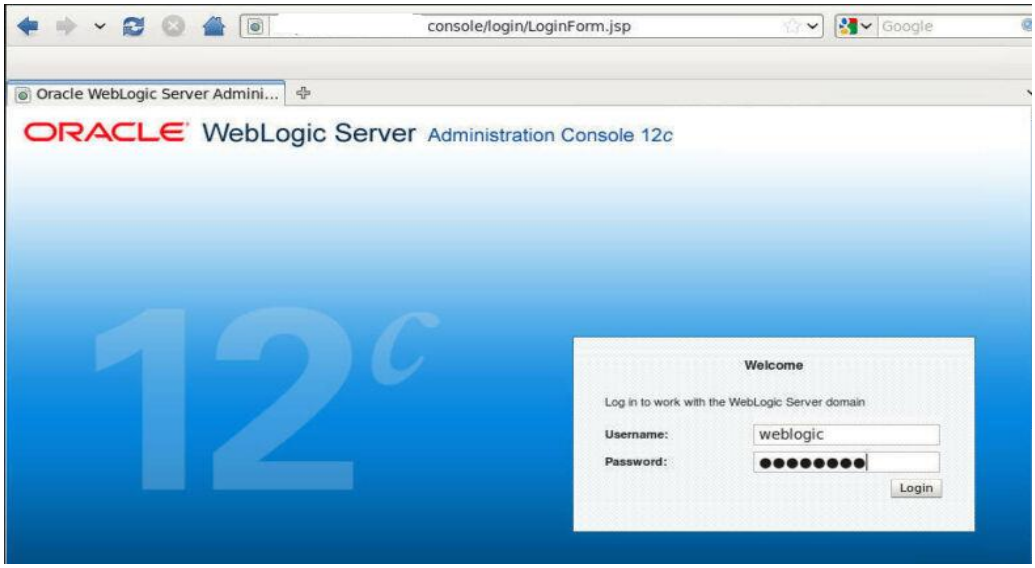
Name: Critical Oracle WebLogic Vulnerability exploited by DarkIRC Malware

Threat Classification: Malware

Affected Products: Oracle WebLogic Server 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, and 14.1.1.0.0.

Summary:

It has been reported that a DarkIRC botnet is actively targeting thousands of exposed Oracle WebLogic servers by exploiting the recently patched critical remote code execution (RCE) vulnerability CVE-2020-14882 that may allow to execute code, including malware which makes the servers part of a botnet that steals passwords and other sensitive information.



For more technical details and analysis, please visit following links:
https://www.bleepingcomputer.com/news/security/critical-oracle-weblogic-flaw-actively-exploited-by-darkirc-malware/

Recommendations:

- It is highly recommended to follow the Oracle provided WebLogic Server security hardening guidelines to remediate the aforementioned critical vulnerability using following official link: https://docs.oracle.com/en/middleware/standalone/weblogic-server/14.1.1.0/lockd/secure.html#GUID-8C0CC8CF-3D16-4DC1-BF54-1C1B17D2CEF8
- Update all software including Operating Systems, Servers, web browsers etc. to the latest and stable versions with appropriate patches.
- Ensure the principle of least privilege and disable unnecessary services/ ports as malware often exploit such services.
- Maintain and implement a strong password policy throughout the infrastructure.
- Regularly maintain data backups and also ensure that backups are stored offline at a secure site.
- Install, regularly maintain and update Antivirus solution from a well reputed vendor.
- Regularly provide Cyber security awareness trainings to employees.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.