

Fix What Matters to Your Business

Summary of Vulnerabilities & Threats

19–25 September 2022

The third week of September 2022 witnessed the discovery of 583 vulnerabilities out of which 6 gained the attention of Threat Actors and security researchers worldwide. Among these 6, there was 2 zero-day. Hive Pro Threat Research Team has curated a list of 6 CVEs that require immediate action.

This week also witnessed the exploitation of two-year-old remote code execution vulnerabilities in Oracle WebLogic Server to deploy Kinsing malware.

Further, we also observed 1 Threat Actor groups being highly active in the last week. UNC4034 , a North Korean threat actor, popular for financial gain that used a fake job posting to lure victims into downloading a trojanized version of PuTTY . Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section.

| Published Vulnerabilities | Interesting Vulnerabilities | Active Threat Groups | Targeted Countries | Targeted Industries | ATT&CK TTPs |
|---------------------------|-----------------------------|----------------------|--------------------|---------------------|-------------|
| 583 | 6 | 1 | Worldwide | 10 | 54 |

Detailed Report

🔧 Interesting Vulnerabilities


| VENDOR | CVE | PATCH DETAILS |
|---|----------------------------------|---|
|  | CVE-2020-14882 CVE-2020-14883 | https://www.oracle.com/security-alerts/cpuoct2020.html |
|  | CVE-2022-3180* | Patch Awaiting |
|  | CVE-2022-37972* | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37972 |
|  | CVE-2022-26134 CVE-2021-4034 | https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html https://gitlab.freedesktop.org/polkit/polkit/-/commit/a2bf5c9c83b6ae46cbd5c779d3055bff81ded683 https://www.debian.org/security/2022/dsa-5059 http://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.434679 https://www.suse.com/support/update/announcement/2022/suse-su-20220189-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20220190-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20220191-1/ https://www.debian.org/lts/security/2022/dla-2899 https://oss.oracle.com/pipermail/el-errata/2022-January/012089.html https://oss.oracle.com/pipermail/el-errata/2022-January/012086.html https://oss.oracle.com/pipermail/el-errata/2022-January/012084.html |

* zero-day vulnerability

Active Actors

| ICON | NAME | ORIGIN | MOTIVE |
|---|---------|-------------|--|
|  | UNC4034 | North Korea | Financial gain & Information theft and espionage |

Targeted Locations

| Color | Targeted By |
|---|-------------|
|  | UNC4034 |

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Targeted Industries



Aerospace



Energy



Financial



Transportation



Media



Defence



Technology



Engineering



Cryptocurrency



Government

Common MITRE ATT&CK TTPs

| TA0043: Reconnaissance | TA0042: Resource Development | TA0001: Initial Access | TA0002: Execution | TA0003: Persistence | TA0004: Privilege Escalation |
|--|-------------------------------------|--|---|---------------------------------------|--|
| T1594: Search Victim-Owned Websites | T1584: Compromise Infrastructure | T1566: Phishing | T1059: Command and Scripting Interpreter | T1574: Hijack Execution Flow | T1548: Abuse Elevation Control Mechanism |
| | T1586: Compromise Accounts | T1566.001: Spearphishing Attachment | T1059.003: Windows Command Shell | T1574.001: DLL Search Order Hijacking | T1574: Hijack Execution Flow |
| | | T1566.003: Spearphishing via Service | T1059.004: Unix Shell | T1053: Scheduled Task/Job | T1574.007: Path Interception by PATH Environment Variable |
| | | T1190: Exploit Public-Facing Application | T1053: Scheduled Task/Job | T1053.005: Scheduled Task | T1053: Scheduled Task/Job |
| | | | T1053.005: Scheduled Task | T1053.003: Cron | T1053.005: Scheduled Task |
| | | | T1053.003: Cron | | T1053.003: Cron |

| TA0005: Defense Evasion | TA0006: Credential Access | TA0007: Discovery | TA0008: Lateral Movement | TA0011: Command and Control | TA0040: Impact |
|--|---|-------------------------------------|--|------------------------------------|---------------------------|
| T1574: Process Injection | T1555: Credentials from Password Stores | T1518: Software Discovery | T1210: Exploitation of Remote Services | T1071: Application Layer Protocol | T1496: Resource Hijacking |
| T1574.001: Dynamic-link Library Injection | T1555.004: Windows Credential Manager | T1082: System Information Discovery | T1021: Remote Services | T1071.001: Web Protocols | T1565: Data Manipulation |
| T1218: System Binary Proxy Execution | T1557: Adversary-in-the-Middle | T1018: Remote System Discovery | | T1071.002: File Transfer Protocols | |
| T1620: Reflective Code Loading | | | | T1132: Data Encoding | |
| T1027: Obfuscated Files or Information | | | | T1132.001: Standard Encoding | |
| T1027.002: Software Packing | | | | T1132.001: Standard Encoding | |
| T1070: Indicator Removal on Host | | | | T1573: Encrypted Channel | |
| T1070.002: Clear Linux or MacSystem Logs | | | | T1573.002: Asymmetric Cryptography | |
| T1070.004: File Deletion | | | | T1573.001: Symmetric Cryptography | |
| T1222: File and Directory Permissions Modification | | | | | |
| T1222.002: Linux and Mac File and Directory Permissions Modification | | | | | |
| T1562: Impair Defenses | | | | | |
| T1562.004: Disable or Modify System Firewall | | | | | |
| T1562.008: Disable Cloud Logs | | | | | |
| T1564: Hide Artifacts | | | | | |
| T1564.001: Hidden Files and Directories | | | | | |



Threat Advisories

<https://www.hivepro.com/unc4034-slips-in-a-backdoor-with-trojanized-putty/>

<https://www.hivepro.com/kinsing-malware-continues-to-exploit-these-two-year-old-vulnerabilities/>

<https://www.hivepro.com/zero-day-vulnerability-in-wpgateway-plugin-compromises-wordpress-sites/>

<https://www.hivepro.com/zero-day-vulnerability-in-windows-terminal-management-tool-gets-a-hotfix/>

<https://www.hivepro.com/vulnerable-atlassian-confluence-servers-utilized-to-drop-crypto-miners/>

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

September 26, 2022 • 4:58 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com