BULLETIN (SB20-335)
VULNERABILITY SUMMARY FOR THE MONTH OF NOVEMBER 20

Bulletin (SB20-335)
Vulnerability Summary for the month of November 2020

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis . The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration.	2020-11-24	10	CVE-2020-29056 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. It allows remote attackers to cause a denial of service (reboot) by sending random bytes to the telnet server on port 23, aka a "shawarma" attack.	2020-11-24	7.8	CVE-2020-29057 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware.	2020-11-24	7.5	CVE-2020-29059 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account.	2020-11-24	7.5	CVE-2020-29060 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account.	2020-11-24	7.5	CVE-2020-29061 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account.	2020-11-24	7.5	CVE-2020-29062 MISC
craftercms -- crafter_cms	In Crafter CMS Crafter Studio 3.0.1 a directory traversal vulnerability exists which allows unauthenticated attackers to overwrite files from the operating system which can lead to RCE.	2020-11-27	7.5	CVE-2017-15681 MISC MISC
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 thorugh 10.1.6 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 190454.	2020-11-23	7.5	CVE-2020-4854 XF CONFIRM

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
newsscriptphp -- news_script_php_pro	SimplePHPscripts News Script PHP Pro 2.3 is affected by a SQL Injection via the id parameter in an editNews action.	2020-11-24	7.5	CVE-2020-25475 MISC MISC
pcanalyser -- pc_analyser	An issue was discovered in Devid Espenschied PC Analyser through 4.10. The PCADRVX64.SYS kernel driver exposes IOCTL functionality that allows low-privilege users to read and write to arbitrary Model Specific Registers (MSRs). This could lead to arbitrary Ring-0 code execution and escalation of privileges.	2020-11-27	7.2	CVE-2020-28921 MISC MISC MISC
pcanalyser -- pc_analyser	An issue was discovered in Devid Espenschied PC Analyser through 4.10. The PCADRVX64.SYS kernel driver exposes IOCTL functionality that allows low-privilege users to read and write arbitrary physical memory. This could lead to arbitrary Ring-0 code execution and escalation of privileges.	2020-11-27	7.2	CVE-2020-28922 MISC MISC MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bigbluebutton -- bigbluebutton	An issue was discovered in BigBlueButton through 2.2.29. A brute-force attack may occur because an unlimited number of codes can be entered for a meeting that is protected by an access code.	2020-11-26	4.3	CVE-2020-29042 MISC MISC MISC
bigbluebutton -- bigbluebutton	An issue was discovered in BigBlueButton through 2.2.29. When at attacker is able to view an account_activations/edit?token= URI, the attacker can create an approved user account associated with an email address that has an arbitrary domain name.	2020-11-26	5	CVE-2020-29043 MISC MISC MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests.	2020-11-24	5	CVE-2020-29058 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. By default, the appliance can be managed remotely only with HTTP, telnet, and SNMP. It doesn't support SSL/TLS for HTTP or SSH. An attacker can intercept passwords sent in cleartext and conduct man-in-the-middle attacks on the management of the appliance.	2020-11-24	4.3	CVE-2020-29055 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. A custom encryption algorithm is used to store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value.	2020-11-24	5	CVE-2020-29063 MISC
cdata -- 72408a_firmware	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN, FD1108S, FD1204S-R2, FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials.	2020-11-24	5	CVE-2020-29054 MISC
craftercms -- crafter_cms	Crafter CMS Crafter Studio 3.0.1 has a directory traversal vulnerability which allows unauthenticated attackers to view files from the operating system.	2020-11-27	5	CVE-2017-15684 MISC MISC
craftercms -- crafter_cms	Crafter CMS Crafter Studio 3.0.1 is affected by: XML External Entity (XXE). An unauthenticated attacker is able to create a site with specially crafted XML that allows the retrieval of OS files out-of-band.	2020-11-27	5	CVE-2017-15685 MISC MISC
craftercms -- crafter_cms	In Crafter CMS Crafter Studio 3.0.1 an unauthenticated attacker is able to create a site with specially crafted XML that allows the retrieval of OS files out-of-band.	2020-11-27	5	CVE-2017-15683

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
craftercms -- crafter_cms	In Crafter CMS Crafter Studio 3.0.1 an unauthenticated attacker is able to inject malicious JavaScript code resulting in a stored/blind XSS in the admin panel.	2020-11-27	4.3	CVE-2017-15682 MISC MISC
craftercms -- crafter_cms	Crafter CMS Crafter Studio 3.0.1 is affected by: Cross Site Scripting (XSS), which allows remote attackers to steal users' cookies.	2020-11-27	4.3	CVE-2017-15686 MISC
craftercms -- crafter_cms	In Crafter CMS Crafter Studio 3.0.1 an IDOR vulnerability exists which allows unauthenticated attackers to view and modify administrative data.	2020-11-27	6.4	CVE-2017-15680 MISC MISC
glpi-project -- glpi	In GLPI before 9.5.3, ajax/getDropdownValue.php has an Insecure Direct Object Reference (IDOR) vulnerability that allows an attacker to read data from any itemType (e.g., Ticket, Users, etc.).	2020-11-26	4	CVE-2020-27663 MISC
glpi-project -- glpi	In GLPI before 9.5.3, ajax/comments.php has an Insecure Direct Object Reference (IDOR) vulnerability that allows an attacker to read data from any database table (e.g., glpi_tickets, glpi_users, etc.).	2020-11-26	4	CVE-2020-27662 MISC
hrsale -- hrsale	HRSALE 2.0.0 allows XSS via the admin/project/projects_calendar set_date parameter.	2020-11-24	4.3	CVE-2020-29053 MISC MISC
ibm -- spectrum_control	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 189214.	2020-11-23	4.3	CVE-2020-4783 XF CONFIRM
ibm -- spectrum_protect_operations_center	IBM Spectrum Protect Operations Center 8.1.0.000 through 8.1.10.and 7.1.0.000 through 7.1.11 could allow a remote attacker to obtain sensitive information, caused by improper authentication of a websocket endpoint. By using known tools to subscribe to the websocket event stream, an attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 188993.	2020-11-23	5	CVE-2020-4771 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 191814.	2020-11-20	5	CVE-2020-4937 XF CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted applyOps invocations. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.10; v3.6 versions prior to 3.6.13.	2020-11-23	4	CVE-2018-20804 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may cause denial of service by issuing a specially crafted query which violates an invariant in the server selection subsystem. This issue affects: MongoDB Server version 4.4 prior to 4.4.1. Versions before 4.4 are not affected.	2020-11-23	4	CVE-2020-7926 CONFIRM

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries with compound indexes affecting QueryPlanner. This issue affects: MongoDB Inc. MongoDB Server v3.6 versions prior to 3.6.9, v4.0 versions prior to 4.0.3.	2020-11-23	4	CVE-2018-20802 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use the $mod operator to overflow negative values. This issue affects: MongoDB Inc. MongoDB Server v4.4 versions prior to 4.4.1; v4.2 versions prior to 4.2.9; v4.0 versions prior to 4.0.20; v3.6 versions prior to 3.6.20.	2020-11-23	4	CVE-2019-2392 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which perform an $elemMatch This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.5; v3.6 versions prior to 3.6.10. This issue affects: MongoDB Inc. MongoDB Server 3.6 versions prior to 3.6.10; 4.0 versions prior to 4.0.5.	2020-11-23	4	CVE-2018-20805 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which throw unhandled Javascript exceptions containing types intended to be scoped to the Javascript engine's internals. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.7.	2020-11-23	4	CVE-2019-20923 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries which trigger an invariant in the IndexBoundsBuilder. This issue affects: MongoDB Inc. MongoDB Server v4.2 versions prior to 4.2.2.	2020-11-23	4	CVE-2019-20924 CONFIRM
mongodb -- mongodb	A user authorized to perform database queries may trigger denial of service by issuing specially crafted queries, which use $lookup and collations. This issue affects: MongoDB Inc. MongoDB Server v4.2 versions prior to 4.2.1; v4.0 versions prior to 4.0.13; v3.6 versions prior to 3.6.15.	2020-11-23	4	CVE-2019-2393 CONFIRM
newsscriptphp -- news_script_php_pro	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Scripting (XSS) vulnerability via the editor_name parameter.	2020-11-24	4.3	CVE-2020-25474 MISC MISC MISC
newsscriptphp -- news_script_php_pro	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Request Forgery (CSRF) vulnerability, which allows attackers to add new users.	2020-11-24	4.3	CVE-2020-25472 MISC MISC MISC
tianocore -- edk2	Use after free vulnerability in EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via adjacent access.	2020-11-23	5.2	CVE-2019-14586 MISC
tianocore -- edk2	Logic issue in DxeImageVerificationHandler() for EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-11-23	4.6	CVE-2019-14575 MISC
tianocore -- edk2	Improper authentication in EDK II may allow a privileged user to potentially enable information disclosure via network access.	2020-11-23	4	CVE-2019-14553 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tianocore -- edk2	Integer truncation in EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-11-23	4.6	CVE-2019-14563 MISC
tianocore -- edk2	Uncontrolled resource consumption in EDK II may allow an unauthenticated user to potentially enable denial of service via network access.	2020-11-23	5	CVE-2019-14559 MISC
v-secure -- jingyun_antivirus	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12364020.	2020-11-23	4.6	CVE-2018-16723 MISC MISC
v-secure -- jingyun_antivirus	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12360094, a related issue to CVE-2018-16305.	2020-11-23	4.6	CVE-2018-16722 MISC MISC
v-secure -- jingyun_antivirus	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x12360090, a related issue to CVE-2018-16306.	2020-11-23	4.6	CVE-2018-16721 MISC MISC
v-secure -- jingyun_antivirus	In Jingyun Antivirus v2.4.2.39, the driver file (ZySandbox.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x1236001c, a related issue to CVE-2018-16304.	2020-11-23	4.6	CVE-2018-16720 MISC MISC
v-secure -- jingyun_antivirus	In Jingyun Antivirus v2.4.2.39, the driver file (hookbody.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x00221482.	2020-11-23	4.6	CVE-2018-16719 MISC MISC

LOW Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oscommerce -- oscommerce	osCommerce 2.3.4.1 has XSS vulnerability via the authenticated user entering the XSS payload into the title section of newsletters.	2020-11-25	3.5	CVE-2020-29070 MISC MISC MISC
tianocore -- edk2	Logic issue EDK II may allow an unauthenticated user to potentially enable denial of service via adjacent access.	2020-11-23	3.3	CVE-2019-14587 MISC
tianocore -- edk2	Integer overflow in DxeImageVerificationHandler() EDK II may allow an authenticated user to potentially enable denial of service via local access.	2020-11-23	2.1	CVE-2019-14562 MISC