National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Nov 2020 Vol. 07 No. 22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
aviatrix					
controller					
Insufficiently Protected Credentials	17-Nov-20	5	An issue was discovered in Aviatrix Controller before R5.3.1151. An encrypted file containing credentials to unrelated systems is protected by a three-character key. **CVE ID : CVE-2020-26550**	N/A	A-AVI-CONT-021220/1
Cleartext Storage of Sensitive Information	17-Nov-20	5	An issue was discovered in Aviatrix Controller before R5.3.1151. Encrypted key values are stored in a readable file. **CVE ID : CVE-2020-26551**	N/A	A-AVI-CONT-021220/2
Unrestricted Upload of File with Dangerous Type	17-Nov-20	7.5	An issue was discovered in Aviatrix Controller before R6.0.2483. Several APIs contain functions that allow arbitrary files to be uploaded to the web tree. **CVE ID : CVE-2020-26553**	N/A	A-AVI-CONT-021220/3
bigbluebutton					
bigbluebutton					
Improper Encoding or Escaping of Output	19-Nov-20	5	web/controllers/ApiController.groovy in BigBlueButton before 2.2.29 lacks certain parameter sanitization, as demonstrated by accepting control characters in a user name.	N/A	A-BIG-BIGB-021220/4

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-28954		
Improper Restriction of Excessive Authentication Attempts	26-Nov-20	4.3	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. **CVE ID : CVE-2020-29042**	N/A	A-BIG-BIGB-021220/5
Missing Authorization	26-Nov-20	5	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. **CVE ID : CVE-2020-29043**	N/A	A-BIG-BIGB-021220/6
Chronoengine					
chronoforums					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	4.3	Chronoforeum 2.0.11 allows Stored XSS vulnerabilities when inserting a crafted payload into a post. If any user sees the post, the inserted XSS code is executed. **CVE ID : CVE-2020-27459**	N/A	A-CHR-CHRO-021220/7
Cisco					
roomos					
Authorization Bypass Through User-Controlled Key	18-Nov-20	5.5	A vulnerability in the xAPI service of Cisco Telepresence CE Software and Cisco RoomOS Software could allow an authenticated, remote attacker to generate an access	N/A	A-CIS-ROOM-021220/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			token for an affected device. The vulnerability is due to insufficient access authorization. An attacker could exploit this vulnerability by using the xAPI service to generate a specific token. A successful exploit could allow the attacker to use the generated token to enable experimental features on the device that should not be available to users. **CVE ID : CVE-2020-26068**		
webex_meetings_server					
Improper Input Validation	18-Nov-20	5	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to view sensitive information from the meeting room lobby. This vulnerability is due to insufficient protection of sensitive participant information. An attacker could exploit this vulnerability by browsing the Webex roster. A successful exploit could allow the attacker to gather information about other Webex participants, such as email address and IP address, while waiting in the lobby. **CVE ID : CVE-2020-3441**	N/A	A-CIS-WEBE-021220/9
Improper Input Validation	18-Nov-20	5	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to maintain bidirectional audio despite	N/A	A-CIS-WEBE-021220/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			being expelled from an active Webex session. The vulnerability is due to a synchronization issue between meeting and media services on a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. A successful exploit could allow the attacker to maintain the audio connection of a Webex session despite being expelled. **CVE ID : CVE-2020-3471**		
iot_field_network_director					
Improper Privilege Management	18-Nov-20	5.5	A vulnerability in the SOAP API of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to access and modify information on devices that belong to a different domain. The vulnerability is due to insufficient authorization in the SOAP API. An attacker could exploit this vulnerability by sending SOAP API requests to affected devices for devices that are outside their authorized domain. A successful exploit could allow the attacker to access and modify information on devices that belong to a different domain. **CVE ID : CVE-2020-26072**	N/A	A-CIS-IOT_-021220/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Nov-20	9	A vulnerability in the REST API of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to gain access to the back-end database of an affected device. The vulnerability is due to insufficient input validation of REST API requests that are made to an affected device. An attacker could exploit this vulnerability by crafting malicious API requests to the affected device. A successful exploit could allow the attacker to gain access to the back-end database of the affected device. **CVE ID : CVE-2020-26075**	N/A	A-CIS-IOT_-021220/12
Information Exposure	18-Nov-20	5	A vulnerability in Cisco IoT Field Network Director (FND) could allow an unauthenticated, remote attacker to view sensitive database information on an affected device. The vulnerability is due to the absence of authentication for sensitive information. An attacker could exploit this vulnerability by sending crafted curl commands to an affected device. A successful exploit could allow the attacker to view sensitive database information on the affected device. **CVE ID : CVE-2020-26076**	N/A	A-CIS-IOT_-021220/13
Improper Privilege	18-Nov-20	4	A vulnerability in the access control functionality of Cisco	N/A	A-CIS-IOT_-021220/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			IoT Field Network Director (FND) could allow an authenticated, remote attacker to view lists of users from different domains that are configured on an affected system. The vulnerability is due to improper access control. An attacker could exploit this vulnerability by sending an API request that alters the domain for a requested user list on an affected system. A successful exploit could allow the attacker to view lists of users from different domains on the affected system. **CVE ID : CVE-2020-26077**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Nov-20	5.5	A vulnerability in the file system of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to overwrite files on an affected system. The vulnerability is due to insufficient file system protections. An attacker could exploit this vulnerability by crafting API requests and sending them to an affected system. A successful exploit could allow the attacker to overwrite files on an affected system. **CVE ID : CVE-2020-26078**	N/A	A-CIS-IOT_-021220/15
Insufficiently Protected Credentials	18-Nov-20	4	A vulnerability in the web UI of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker	N/A	A-CIS-IOT_-021220/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to obtain hashes of user passwords on an affected device. The vulnerability is due to insufficient protection of user credentials. An attacker could exploit this vulnerability by logging in as an administrative user and crafting a call for user information. A successful exploit could allow the attacker to obtain hashes of user passwords on an affected device. **CVE ID : CVE-2020-26079**		
Improper Privilege Management	18-Nov-20	4	A vulnerability in the user management functionality of Cisco IoT Field Network Director (FND) could allow an authenticated, remote attacker to manage user information for users in different domains on an affected system. The vulnerability is due to improper domain access control. An attacker could exploit this vulnerability by manipulating JSON payloads to target different domains on an affected system. A successful exploit could allow the attacker to manage user information for users in different domains on an affected system. **CVE ID : CVE-2020-26080**	N/A	A-CIS-IOT_-021220/17
Improper Neutralization of Special Elements in	18-Nov-20	4.3	Multiple vulnerabilities in the web UI of Cisco IoT Field Network Director (FND) could allow an unauthenticated,	N/A	A-CIS-IOT_-021220/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			remote attacker to conduct cross-site scripting (XSS) attacks against users on an affected system. The vulnerabilities are due to insufficient validation of user-supplied input that is processed by the web UI. An attacker could exploit these vulnerabilities by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information on an affected system. **CVE ID : CVE-2020-26081**		
webex_meetings					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	4.3	A vulnerability in an API of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to improper validation of user-supplied input to an application programmatic interface (API) within Cisco Webex Meetings. An attacker could exploit this vulnerability by convincing a targeted user to follow a link designed to submit malicious input to the API used by Cisco Webex Meetings. A successful exploit could allow the attacker to conduct cross-site scripting attacks and potentially gain	N/A	A-CIS-WEBE-021220/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive browser-based information from the system of a targeted user. **CVE ID : CVE-2020-27126**		
Improper Input Validation	18-Nov-20	5	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to view sensitive information from the meeting room lobby. This vulnerability is due to insufficient protection of sensitive participant information. An attacker could exploit this vulnerability by browsing the Webex roster. A successful exploit could allow the attacker to gather information about other Webex participants, such as email address and IP address, while waiting in the lobby. **CVE ID : CVE-2020-3441**	N/A	A-CIS-WEBE-021220/20
telepresence_collaboration_endpoint					
Authorization Bypass Through User-Controlled Key	18-Nov-20	5.5	A vulnerability in the xAPI service of Cisco Telepresence CE Software and Cisco RoomOS Software could allow an authenticated, remote attacker to generate an access token for an affected device. The vulnerability is due to insufficient access authorization. An attacker could exploit this vulnerability by using the xAPI service to generate a specific token. A successful exploit could allow the attacker to use the generated token to enable	N/A	A-CIS-TELE-021220/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			experimental features on the device that should not be available to users. **CVE ID : CVE-2020-26068**		
cloudavid					
pparam					
Uncontrolled Resource Consumption	16-Nov-20	5	Memory leak in IPv6Param::setAddress in CloudAvid PParam 1.3.1. **CVE ID : CVE-2020-28723**	N/A	A-CLO-PPAR-021220/22
Gitlab					
gitaly					
Insufficient Session Expiration	17-Nov-20	2.1	When importing repos via URL, one time use git credentials were persisted beyond the expected time window in Gitaly 1.79.0 or above. Affected versions are: >=1.79.0, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2. **CVE ID : CVE-2020-13353**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13353.json	A-GIT-GITA-021220/23
gitlab					
N/A	17-Nov-20	4	An issue has been discovered in GitLab EE affecting all versions starting from 10.2. Required CODEOWNERS approval could be bypassed by targeting a branch without the CODEOWNERS file. Affected versions are >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2. **CVE ID : CVE-2020-13348**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13348.json	A-GIT-GITL-021220/24
N/A	17-Nov-20	4	An issue has been discovered in GitLab EE affecting all versions starting from 8.12. A regular expression related to a	https://gitlab.com/gitlab-org/cves/-	A-GIT-GITL-021220/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file path resulted in the Advanced Search feature susceptible to catastrophic backtracking. Affected versions are >=8.12, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2. **CVE ID : CVE-2020-13349**	/blob/master/2020/CVE-2020-13349.json	
Cross-Site Request Forgery (CSRF)	17-Nov-20	4.3	CSRF in runner administration page in all versions of GitLab CE/EE allows an attacker who's able to target GitLab instance administrators to pause/resume runners. Affected versions are >=13.5.0, <13.5.2,>=13.4.0, <13.4.5,<13.3.9. **CVE ID : CVE-2020-13350**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13350.json	A-GIT-GITL-021220/26
Incorrect Default Permissions	17-Nov-20	5	Insufficient permission checks in scheduled pipeline API in GitLab CE/EE 13.0+ allows an attacker to read variable names and values for scheduled pipelines on projects visible to the attacker. Affected versions are >=13.0, <13.3.9,>=13.4.0, <13.4.5,>=13.5.0, <13.5.2. **CVE ID : CVE-2020-13351**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13351.json	A-GIT-GITL-021220/27
N/A	17-Nov-20	5	Private group info is leaked leaked in GitLab CE/EE version 10.2 and above, when the project is moved from private to public group. Affected versions are: >=10.2, <13.3.9,>=13.4, <13.4.5,>=13.5, <13.5.2. **CVE ID : CVE-2020-13352**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13352.json	A-GIT-GITL-021220/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	17-Nov-20	2.1	A vulnerability in the internal Kubernetes agent api in GitLab CE/EE version 13.3 and above allows unauthorized access to private projects. Affected versions are: >=13.4, <13.4.5,>=13.3, <13.3.9,>=13.5, <13.5.2. **CVE ID : CVE-2020-13358**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13358.json	A-GIT-GITL-021220/29
Glpi-project					
glpi					
Insecure Storage of Sensitive Information	26-Nov-20	4	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.). **CVE ID : CVE-2020-27662**	N/A	A-GLP-GLPI-021220/30
Insecure Storage of Sensitive Information	26-Nov-20	4	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.). **CVE ID : CVE-2020-27663**	N/A	A-GLP-GLPI-021220/31
Golang					
go					
Improper Certificate Validation	18-Nov-20	5	Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service. **CVE ID : CVE-2020-28362**	https://groups.google.com/g/golang-nuts/c/c-ssaaS7RMI	A-GOL-GO-021220/32
Improper Control of	18-Nov-20	5.1	Go before 1.14.12 and 1.15.x before 1.15.5 allows Code	https://groups.googl	A-GOL-GO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			Injection. **CVE ID : CVE-2020-28366**	e.com/g/golang-announce/c/NpBGTTmKzpM	021220/33
Argument Injection or Modification	18-Nov-20	5.1	Go before 1.14.12 and 1.15.x before 1.15.5 allows Argument Injection. **CVE ID : CVE-2020-28367**	https://groups.google.com/g/golang-announce/c/NpBGTTmKzpM	A-GOL-GO-021220/34
grocy_project					
grocy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	3.5	Cross-site Scripting (XSS) vulnerability in grocy 2.7.1 via the add recipe module, which gets executed when deleting the recipe. **CVE ID : CVE-2020-25454**	N/A	A-GRO-GROC-021220/35
gym_management_system_project					
gym_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	4.3	Stored Cross-site scripting (XSS) vulnerability in SourceCodester Gym Management System 1.0 allows users to inject and store arbitrary JavaScript code in index.php?page=packages via vulnerable fields 'Package Name' and 'Description'. **CVE ID : CVE-2020-28129**	N/A	A-GYM-GYM_-021220/36
hrsale					
hrsale					
Improper Neutralizatio	24-Nov-20	4.3	HRSALE 2.0.0 allows XSS via the	N/A	A-HRS-HRSA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			admin/project/projects_calendar set_date parameter. **CVE ID : CVE-2020-29053**		021220/37
IBM					
jazz_reporting_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-20	3.5	IBM Jazz Reporting Service 6.0.6, 6.0.6.1, 7.0, and 7.0.1 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 187731. **CVE ID : CVE-2020-4718**	https://www.ibm.com/support/pages/node/6370099	A-IBM-JAZZ-021220/38
spectrum_protect_operations_center					
Improper Authentication	23-Nov-20	5	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. **CVE ID : CVE-2020-4771**	https://www.ibm.com/support/pages/node/6369101	A-IBM-SPEC-021220/39
sterling_file_gateway					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-20	5	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 181778. **CVE ID : CVE-2020-4476**	https://www.ibm.com/support/pages/node/6367971	A-IBM-STER-021220/40
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Nov-20	6.5	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. **CVE ID : CVE-2020-4647**	https://www.ibm.com/support/pages/node/6367981	A-IBM-STER-021220/41
N/A	16-Nov-20	4.3	IBM Sterling File Gateway 2.2.0.0 through 2.2.6.5 and 6.0.0.0 through 6.0.3.2 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 186280. **CVE ID : CVE-2020-4665**	https://www.ibm.com/support/pages/node/6367997	A-IBM-STER-021220/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Nov-20	4.3	IBM Sterling File Gateway 6.0.0.0 through 6.0.3.2 and 2.2.0.0 through 2.2.6.5 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 188897. **CVE ID : CVE-2020-4763**	https://www.ibm.com/support/pages/node/6368025	A-IBM-STER-021220/43
spectrum_protect_plus					
Use of Hard-coded Credentials	23-Nov-20	7.5	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. **CVE ID : CVE-2020-4854**	https://www.ibm.com/support/pages/node/6367823	A-IBM-SPEC-021220/44
sterling_b2b_integrator					
N/A	16-Nov-20	4	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 5.2.6.5 and 6.0.0.0 through 6.0.3.2 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information	https://www.ibm.com/support/pages/node/6367963	A-IBM-STER-021220/45

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could be used in further attacks against the system. **CVE ID : CVE-2020-4475**		
N/A	16-Nov-20	4	IBM Sterling B2B Integrator Standard Edition 5.2.6.0 through 5.2.6.5 and 6.0.0.0 through 6.0.3.2 stores potentially highly sensitive information in log files that could be read by an authenticated user. IBM X-Force ID: 184083. **CVE ID : CVE-2020-4566**	https://www.ibm.com/support/pages/node/6367975	A-IBM-STER-021220/46
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Nov-20	6.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 186091. **CVE ID : CVE-2020-4655**	https://www.ibm.com/support/pages/node/6367995	A-IBM-STER-021220/47
Information Exposure Through Log Files	16-Nov-20	4	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 stores potentially sensitive information in log files that could be read by an authenticatedl user. IBM X-Force ID: 186284. **CVE ID : CVE-2020-4671**	https://www.ibm.com/support/pages/node/6368001	A-IBM-STER-021220/48
N/A	16-Nov-20	4	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0	https://www.ibm.com/support	A-IBM-STER-021220/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 5.2.6.5 could allow an authenticated user to obtain sensitive information from the Dashboard UI. IBM X-Force ID: 186780. **CVE ID : CVE-2020-4692**	/pages/node/6368009	
N/A	16-Nov-20	6.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 could allow an authenticated user belonging to a specific user group to create a user or group with administrative privileges. IBM X-Force ID: 187077. **CVE ID : CVE-2020-4700**	https://www.ibm.com/support/pages/node/6367979	A-IBM-STER-021220/50
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.2 and 5.2.0.0 through 5.2.6.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 187190. **CVE ID : CVE-2020-4705**	https://www.ibm.com/support/pages/node/6368013	A-IBM-STER-021220/51
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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.	https://www.ibm.com/support/pages/node/6370795	A-IBM-STER-021220/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4937		
spectrum_control					
Information Exposure	23-Nov-20	4.3	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. **CVE ID : CVE-2020-4783**	https://www.ibm.com/support/pages/node/6368601	A-IBM-SPEC-021220/53
business_automation_workflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	IBM Business Automation Workflow 20.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 186285. **CVE ID : CVE-2020-4672**	https://www.ibm.com/support/pages/node/6367813	A-IBM-BUSI-021220/54
ivanti					
endpoint_manager					
Improper Neutralization of Special Elements used in an SQL Command	16-Nov-20	6.5	LDMS/alert_log.aspx in Ivanti Endpoint Manager through 2020.1 allows SQL Injection via a /remotecontrolauth/api/device request. **CVE ID : CVE-2020-13769**	N/A	A-IVA-ENDP-021220/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')					
N/A	16-Nov-20	5	In /ldclient/ldprov.cgi in Ivanti Endpoint Manager through 2020.1.1, an attacker is able to disclose information about the server operating system, local pathnames, and environment variables with no authentication required. **CVE ID : CVE-2020-13772**	N/A	A-IVA-ENDP-021220/56
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Ivanti Endpoint Manager through 2020.1.1 allows XSS via /LDMS/frm_splitfrm.aspx, /LDMS/licensecheck.aspx, /LDMS/frm_splitcollapse.aspx, /LDMS/alert_log.aspx, /LDMS/ServerList.aspx, /LDMS/frm_coremainfrm.aspx, /LDMS/frm_findfrm.aspx, /LDMS/frm_taskfrm.aspx, and /LDMS/query_browsecomp.aspx. **CVE ID : CVE-2020-13773**	N/A	A-IVA-ENDP-021220/57
Jetbrains					
youtrack					
Server-Side Request Forgery (SSRF)	16-Nov-20	5	JetBrains YouTrack before 2020.3.888 was vulnerable to SSRF. **CVE ID : CVE-2020-27624**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-YOUT-021220/58
N/A	16-Nov-20	5	In JetBrains YouTrack before 2020.3.888, notifications might have mentioned inaccessible issues.	N/A	A-JET-YOUT-021220/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27625		
Server-Side Request Forgery (SSRF)	16-Nov-20	5	JetBrains YouTrack before 2020.3.5333 was vulnerable to SSRF. **CVE ID : CVE-2020-27626**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-YOUT-021220/60
Information Exposure	16-Nov-20	2.1	Sensitive information could be disclosed in the JetBrains YouTrack application before 2020.2.0 for Android via application backups. **CVE ID : CVE-2020-24366**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-YOUT-021220/61
Information Exposure	16-Nov-20	5	In JetBrains YouTrack before 2020.3.6638, improper access control for some subresources leads to information disclosure via the REST API. **CVE ID : CVE-2020-25209**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-YOUT-021220/62
Information Exposure	16-Nov-20	5	In JetBrains YouTrack before 2020.3.7955, an attacker could access workflow rules without appropriate access grants. **CVE ID : CVE-2020-25210**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-YOUT-021220/63
toolbox					
N/A	16-Nov-20	5	JetBrains ToolBox before version 1.18 is vulnerable to a Denial of Service attack via a browser protocol handler. **CVE ID : CVE-2020-25013**	https://blog.jetbrains.com/2020/11/16/jetbrains-	A-JET-TOOL-021220/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				security-bulletin-q3-2020/	
N/A	16-Nov-20	10	JetBrains ToolBox before version 1.18 is vulnerable to Remote Code Execution via a browser protocol handler. **CVE ID : CVE-2020-25207**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-TOOL-021220/65
intellij_idea					
N/A	16-Nov-20	5	In JetBrains IntelliJ IDEA before 2020.2, the built-in web server could expose information about the IDE version. **CVE ID : CVE-2020-27622**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-INTE-021220/66
teamcity					
N/A	16-Nov-20	4	In JetBrains TeamCity before 2020.1.5, the Guest user had access to audit records. **CVE ID : CVE-2020-27628**	https://blog.jetbrains.com/2020/11/16/jetbrains-security-bulletin-q3-2020/	A-JET-TEAM-021220/67
kaaproject					
kaa					
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Nov-20	3.5	Cross-site scripting (XSS) vulnerability in Dashboards section in Kaa IoT Platform v1.2.0 allows remote attackers to inject malicious web scripts or HTML Injection payloads via the Description parameter.	N/A	A-KAA-KAA-021220/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2020-26701**		
Limesurvey					
limesurvey					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	3.5	A stored cross-site scripting (XSS) vulnerability in LimeSurvey before and including 3.21.1 allows authenticated users with correct permissions to inject arbitrary web script or HTML via parameter ParticipantAttributeNamesDropdown of the Attributes on the central participant database page. When the survey attribute being edited or viewed, e.g. by an administrative user, the JavaScript code will be executed in the browser. **CVE ID : CVE-2020-25798**	N/A	A-LIM-LIME-021220/69
ljcmsshop_project					
ljcmsshop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	4.3	A cross-site scripting (XSS) vulnerability in Beijing Liangjing Zhicheng Technology Co., Ltd ljcmsshop version 1.14 allows remote attackers to inject arbitrary web script or HTML via user.php by registering an account directly in the user center, and then adding the payload to the delivery address. **CVE ID : CVE-2020-22723**	N/A	A-LJC-LJCM-021220/70
Microfocus					
arcsight_logger					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	4.3	Cross-Site Scripting vulnerability on Micro Focus ArcSight Logger product, affecting all version prior to 7.1.1. The vulnerability could be remotely exploited resulting in Cross-Site Scripting (XSS) **CVE ID : CVE-2020-11860**	https://community.microfocus.com/t5/Logger/Logger-Release-Notes-7-1-1/ta-p/2837600	A-MIC-ARCS-021220/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	4.3	Cross-Site Scripting vulnerability on Micro Focus ArcSight Logger product, affecting version 7.1. The vulnerability could be remotely exploited resulting in Cross-Site Scripting (XSS). **CVE ID : CVE-2020-25834**	https://community.microfocus.com/t5/Logger/Logger-Release-Notes-7-1-1/ta-p/2837600	A-MIC-ARCS-021220/72
idol					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	3.5	Persistent cross-Site Scripting vulnerability on Micro Focus IDOL product, affecting all version prior to version 12.7. The vulnerability could be exploited to perform Persistent XSS attack. **CVE ID : CVE-2020-25833**	https://softwaresupport.softwaregrp.com/doc/KM03763397	A-MIC-IDOL-021220/73
filr					
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Nov-20	3.5	Reflected Cross Site scripting vulnerability on Micro Focus Filr product, affecting version 4.2.1. The vulnerability could be exploited to perform Reflected XSS attack. **CVE ID : CVE-2020-25832**	https://softwaresupport.softwaregrp.com/doc/KM03763396	A-MIC-FILR-021220/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Mongodb					
mongodb					
Improper Handling of Exceptional Conditions	23-Nov-20	4	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. **CVE ID : CVE-2020-7926**	https://jira.mongodb.org/browse/SERVER-50170	A-MON-MONG-021220/75
Nagios					
nagios_xi					
Improper Input Validation	16-Nov-20	6.5	Improper input validation in the Auto-Discovery component of Nagios XI before 5.7.5 allows an authenticated attacker to execute remote code. **CVE ID : CVE-2020-28648**	N/A	A-NAG-NAGI-021220/76
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Nagios XI before 5.7.5 is vulnerable to XSS in Manage Users (Username field). **CVE ID : CVE-2020-27988**	https://www.nagios.com/downloads/nagios-xi/change-log/	A-NAG-NAGI-021220/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Nagios XI before 5.7.5 is vulnerable to XSS in Dashboard Tools (Edit Dashboard). **CVE ID : CVE-2020-27989**	https://www.nagios.com/downloads/nagios-xi/change-log/	A-NAG-NAGI-021220/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Nagios XI before 5.7.5 is vulnerable to XSS in the Deployment tool (add agent). **CVE ID : CVE-2020-27990**	https://www.nagios.com/downloads/nagios-xi/change-log/	A-NAG-NAGI-021220/79
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Nagios XI before 5.7.5 is vulnerable to XSS in Account Information (Email field). **CVE ID : CVE-2020-27991**	https://www.nagios.com/downloads/nagios-xi/change-log/	A-NAG-NAGI-021220/80
newsscriptphp					
news_script_php_pro					
Cross-Site Request Forgery (CSRF)	24-Nov-20	4.3	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Request Forgery (CSRF) vulnerability, which allows attackers to add new users. **CVE ID : CVE-2020-25472**	N/A	A-NEW-NEWS-021220/81
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Nov-20	4.3	SimplePHPscripts News Script PHP Pro 2.3 is affected by a Cross Site Scripting (XSS) vulnerability via the editor_name parameter. **CVE ID : CVE-2020-25474**	N/A	A-NEW-NEWS-021220/82
Improper Neutralization of Special Elements used in an SQL	24-Nov-20	7.5	SimplePHPscripts News Script PHP Pro 2.3 is affected by a SQL Injection via the id parameter in an editNews action.	N/A	A-NEW-NEWS-021220/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2020-25475**		
Nextcloud					
nextcloud					
Insufficiently Protected Credentials	16-Nov-20	2.1	Insufficient protection of the server-side encryption keys in Nextcloud Server 19.0.1 allowed an attacker to replace the public key to decrypt them later on. **CVE ID : CVE-2020-8152**	N/A	A-NEX-NEXT-021220/84
social					
Improper Certificate Validation	19-Nov-20	5.8	Missing validation of server certificates for out-going connections in Nextcloud Social < 0.4.0 allowed a man-in-the-middle attack. **CVE ID : CVE-2020-8279**	https://nextcloud.com/security/advisory/?id=NC-SA-2020-043	A-NEX-SOCI-021220/85
Nodejs					
node.js					
Uncontrolled Resource Consumption	19-Nov-20	5	A Node.js application that allows an attacker to trigger a DNS request for a host of their choice could trigger a Denial of Service in versions < 15.2.1, < 14.15.1, and < 12.19.1 by getting the application to resolve a DNS record with a larger number of responses. This is fixed in 15.2.1, 14.15.1, and 12.19.1. **CVE ID : CVE-2020-8277**	https://nodejs.org/en/blog/vulnerability/november-2020-security-releases/	A-NOD-NODE-021220/86
online_clothing_store_project					
online_clothing_store					
Improper	17-Nov-20	7.5	SourceCodester Online	N/A	A-ONL-ONLI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			Clothing Store 1.0 is affected by a SQL Injection via the txtUserName parameter to login.php. **CVE ID : CVE-2020-28138**		021220/87
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	4.3	SourceCodester Online Clothing Store 1.0 is affected by a cross-site scripting (XSS) vulnerability via a Offer Detail field in offer.php. **CVE ID : CVE-2020-28139**	N/A	A-ONL-ONLI-021220/88
Unrestricted Upload of File with Dangerous Type	17-Nov-20	7.5	SourceCodester Online Clothing Store 1.0 is affected by an arbitrary file upload via the image upload feature of Products.php. **CVE ID : CVE-2020-28140**	N/A	A-ONL-ONLI-021220/89
online_library_management_system_project					
online_library_management_system					
Unrestricted Upload of File with Dangerous Type	17-Nov-20	10	An Arbitrary File Upload in the Upload Image component in SourceCodester Online Library Management System 1.0 allows the user to conduct remote code execution via admin/borrower/index.php?view=add because .php files can be uploaded to admin/borrower/photos (under the web root). **CVE ID : CVE-2020-28130**	N/A	A-ONL-ONLI-021220/90
orbisius					
child_theme_creator					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	16-Nov-20	6.8	The orbisius-child-theme-creator plugin before 1.5.2 for WordPress allows CSRF via orbisius_ctc_theme_editor_manage_file. **CVE ID : CVE-2020-28649**	N/A	A-ORB-CHIL-021220/91
Oscommerce					
oscommerce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Nov-20	3.5	osCommerce 2.3.4.1 has XSS vulnerability via the authenticated user entering the XSS payload into the title section of newsletters. **CVE ID : CVE-2020-29070**	N/A	A-OSC-OSCO-021220/92
pcanalyser					
pc_analyser					
Improper Privilege Management	27-Nov-20	7.2	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. **CVE ID : CVE-2020-28921**	N/A	A-PCA-PC_A-021220/93
Improper Privilege Management	27-Nov-20	7.2	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	N/A	A-PCA-PC_A-021220/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			physical memory. This could lead to arbitrary Ring-0 code execution and escalation of privileges. **CVE ID : CVE-2020-28922**		
phpgurukul					
user_registration_\&_login_and_user_management_system_with_admin_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	3.5	Cross Site Scripting (XSS) vulnerability in the Registration page of the admin panel in PHPGurukul User Registration & Login and User Management System With admin panel 2.1. **CVE ID : CVE-2020-24723**	N/A	A-PHP-USER-021220/95
Postgresql					
postgresql					
Use of a Broken or Risky Cryptographic Algorithm	16-Nov-20	6.8	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-25694**	N/A	A-POS-POST-021220/96
Improper	16-Nov-20	6.5	A flaw was found in	N/A	A-POS-POST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-25695**		021220/97
reddoxx					
maildepot					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	4.3	REDDOXX MailDepot 2033 (aka 2.3.3022) allows XSS via an incoming HTML e-mail message. **CVE ID : CVE-2020-26554**	N/A	A-RED-MAIL-021220/98
Redhat					
keycloak					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Nov-20	3.5	A flaw was found in Keycloak before version 12.0.0, where it is possible to add unsafe schemes for the redirect_uri parameter. This flaw allows an attacker to perform a Cross-site scripting attack. **CVE ID : CVE-2020-10776**	N/A	A-RED-KEYC-021220/99
Riken					
xoonips					
Improper Neutralizatio	16-Nov-20	6.5	SQL injection vulnerability in the XooNIps 3.49 and earlier	N/A	A-RIK-XOON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			allows remote authenticated attackers to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2020-5659**		021220/100
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	Reflected cross-site scripting vulnerability in XooNIps 3.49 and earlier allows remote authenticated attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5662**	N/A	A-RIK-XOON-021220/101
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	4	Stored cross-site scripting vulnerability in XooNIps 3.49 and earlier allows remote authenticated attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5663**	N/A	A-RIK-XOON-021220/102
Deserialization of Untrusted Data	16-Nov-20	7.5	Deserialization of untrusted data vulnerability in XooNIps 3.49 and earlier allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-5664**	N/A	A-RIK-XOON-021220/103
salesagility					
suitecrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Nov-20	3.5	SuiteCRM 7.11.13 is affected by stored Cross-Site Scripting (XSS) in the Documents preview functionality. This vulnerability could allow remote authenticated attackers to inject arbitrary web script or HTML.	N/A	A-SAL-SUIT-021220/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14208		
Schneider-electric					
interactive_graphical_scada_system					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Nov-20	6.8	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 and prior that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7550**	N/A	A-SCH-INTE-021220/105
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Nov-20	6.8	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7551**	N/A	A-SCH-INTE-021220/106
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Nov-20	6.8	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7552**	N/A	A-SCH-INTE-021220/107
Out-of-	19-Nov-20	6.8	A CWE-787 Out-of-bounds	N/A	A-SCH-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7553**		021220/108
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-Nov-20	6.8	A CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7554**	N/A	A-SCH-INTE-021220/109
Out-of-bounds Write	19-Nov-20	6.8	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7555**	N/A	A-SCH-INTE-021220/110
Out-of-bounds Write	19-Nov-20	6.8	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7556**	N/A	A-SCH-INTE-021220/111
Out-of-	19-Nov-20	6.8	A CWE-125 Out-of-bounds Read vulnerability exists in	N/A	A-SCH-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7557**		021220/112
Out-of-bounds Write	19-Nov-20	6.8	A CWE-787 Out-of-bounds Write vulnerability exists in IGSS Definition (Def.exe) version 14.0.0.20247 that could cause Remote Code Execution when malicious CGF (Configuration Group File) file is imported to IGSS Definition. **CVE ID : CVE-2020-7558**	N/A	A-SCH-INTE-021220/113
se					
enterprise_server_installer					
Unquoted Search Path or Element	19-Nov-20	4.4	A CWE-428 Windows Unquoted Search Path vulnerability exists in EcoStruxure Building Operation Enterprise Server installer V1.9 - V3.1 and Enterprise Central installer V2.0 - V3.1 that could cause any local Windows user who has write permission on at least one of the subfolders of the Connect Agent service binary path, being able to gain the privilege of the user who started the service. By default, the Enterprise Server and Enterprise Central is always installed at a location requiring Administrator privileges so the vulnerability is only valid if the application has been installed	N/A	A-SE-ENTE-021220/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a non-secure location. **CVE ID : CVE-2020-28209**		
webreports					
Unrestricted Upload of File with Dangerous Type	19-Nov-20	6.5	A CWE-434 Unrestricted Upload of File with Dangerous Type vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to upload arbitrary files due to incorrect verification of user supplied files and achieve remote code execution. **CVE ID : CVE-2020-7569**	N/A	A-SE-WEBR-021220/115
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-20	3.5	A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Stored) vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Cross-Site Scripting stored attack against other WebReport users. **CVE ID : CVE-2020-7570**	N/A	A-SE-WEBR-021220/116
Improper Neutralization of Input During Web Page Generation	19-Nov-20	3.5	A CWE-79 Multiple Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Reflected) vulnerability exists in EcoStruxure Building	N/A	A-SE-WEBR-021220/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Operation WebReports V1.9 - V3.1 that could cause a remote attacker to inject arbitrary web script or HTML due to incorrect sanitization of user supplied data and achieve a Cross-Site Scripting reflected attack against other WebReport users. **CVE ID : CVE-2020-7571**		
Improper Restriction of XML External Entity Reference ('XXE')	19-Nov-20	6.5	A CWE-611 Improper Restriction of XML External Entity Reference vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause an authenticated remote user being able to inject arbitrary XML code and obtain disclosure of confidential data, denial of service, server side request forgery due to improper configuration of the XML parser. **CVE ID : CVE-2020-7572**	N/A	A-SE-WEBR-021220/118
Improper Access Control	19-Nov-20	6.4	A CWE-284 Improper Access Control vulnerability exists in EcoStruxure Building Operation WebReports V1.9 - V3.1 that could cause a remote attacker being able to access a restricted web resources due to improper access control. **CVE ID : CVE-2020-7573**	N/A	A-SE-WEBR-021220/119
sokrates					
sowasql					
Improper Neutralization of Input	19-Nov-20	4.3	A Cross Site Scripting (XSS) vulnerability exists in OPAC in Sokrates SOWA SowaSQL	N/A	A-SOK-SOWA-021220/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			through 5.6.1 via the sowacgi.php typ parameter. **CVE ID : CVE-2020-28350**		
Trendmicro					
interscan_web_security_virtual_appliance					
Out-of-bounds Write	18-Nov-20	7.5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an unauthenticated, remote attacker to send a specially crafted HTTP message and achieve remote code execution with elevated privileges. **CVE ID : CVE-2020-28578**	N/A	A-TRE-INTE-021220/121
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Nov-20	9	A command injection vulnerability in AddVLANItem of Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an authenticated, remote attacker to send specially crafted HTTP messages and execute arbitrary OS commands with elevated privileges. **CVE ID : CVE-2020-28580**	N/A	A-TRE-INTE-021220/122
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-Nov-20	9	A command injection vulnerability in ModifyVLANItem of Trend Micro InterScan Web Security Virtual Appliance 6.5 SP2 could allow an authenticated, remote attacker to send specially crafted HTTP messages and execute arbitrary OS commands with elevated privileges.	N/A	A-TRE-INTE-021220/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-28581		
user_registration_\&_login_and_user_management_system_project					
user_registration_\&_login_and_user_management_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Nov-20	7.5	SQL injection vulnerability in PHPGurukul User Registration & Login and User Management System With admin panel 2.1 allows remote attackers to execute arbitrary SQL commands and bypass authentication. **CVE ID : CVE-2020-25952**	N/A	A-USE-USER-021220/124
wpbakery					
page_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Nov-20	3.5	The WPBakery plugin before 6.4.1 for WordPress allows XSS because it calls kses_remove_filters to disable the standard WordPress XSS protection mechanism for the Author and Contributor roles. **CVE ID : CVE-2020-28650**	N/A	A-WPB-PAGE-021220/125
Yzmcms					
Yzmcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Nov-20	4.3	In YzmCMS v5.5 the member contribution function in the editor contains a cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-22394**	N/A	A-YZM-YZMC-021220/126
Hardware					
cdata					
72408a					
Insufficiently	24-Nov-20	5	An issue was discovered on	N/A	H-CDA-7240-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			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. **CVE ID : CVE-2020-29054**		021220/127
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-7240-021220/128
Improper	24-Nov-20	10	An issue was discovered on	N/A	H-CDA-7240-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		021220/129
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-7240-021220/130
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-7240-021220/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-7240-021220/132
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-7240-021220/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-7240-021220/134
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-7240-021220/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-7240-021220/136
9008a					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9008-021220/137
Cleartext Transmissio	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-9008-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Sensitive Information			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. **CVE ID : CVE-2020-29055**		021220/138
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9008-021220/139
N/A	24-Nov-20	7.8	An issue was discovered on	N/A	H-CDA-9008-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		021220/140
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9008-021220/141
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-9008-021220/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9008-021220/143
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-9008-021220/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9008-021220/145
Inadequate Encryption Strength	24-Nov-20	5	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.	N/A	H-CDA-9008-021220/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29063		
9016a					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9016-021220/147
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-9016-021220/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9016-021220/149
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9016-021220/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9016-021220/151
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9016-021220/152
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	H-CDA-9016-021220/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9016-021220/154
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-9016-021220/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9016-021220/156
92408a					
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-9240-021220/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-9240-021220/158
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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	N/A	H-CDA-9240-021220/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9240-021220/160
Insufficiently Protected Credentials	24-Nov-20	5	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.	N/A	H-CDA-9240-021220/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29058		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9240-021220/162
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9240-021220/163
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B,	N/A	H-CDA-9240-021220/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9240-021220/165
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	H-CDA-9240-021220/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
92416a					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9241-021220/167
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-9241-021220/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9241-021220/169
N/A	24-Nov-20	7.8	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	N/A	H-CDA-9241-021220/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending random bytes to the telnet server on port 23, aka a "shawarma" attack. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9241-021220/171
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9241-021220/172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9241-021220/173
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9241-021220/174
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-9241-021220/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9241-021220/176
9288					
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	H-CDA-9288-021220/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-9288-021220/178
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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,	N/A	H-CDA-9288-021220/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9288-021220/180
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-9288-021220/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9288-021220/182
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9288-021220/183
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-9288-021220/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9288-021220/185
Inadequate Encryption Strength	24-Nov-20	5	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,	N/A	H-CDA-9288-021220/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
97016					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9701-021220/187
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-9701-021220/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9701-021220/189
N/A	24-Nov-20	7.8	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,	N/A	H-CDA-9701-021220/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9701-021220/191
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-9701-021220/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9701-021220/193
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9701-021220/194
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-9701-021220/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9701-021220/196
97024p					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-9702-021220/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-9702-021220/198
Improper Neutralization of Special Elements used in a Command ('Command	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-9702-021220/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9702-021220/200
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	H-CDA-9702-021220/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9702-021220/202
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	H-CDA-9702-021220/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29060		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9702-021220/204
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9702-021220/205
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-9702-021220/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
97028p					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9702-021220/207
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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,	N/A	H-CDA-9702-021220/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9702-021220/209
N/A	24-Nov-20	7.8	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,	N/A	H-CDA-9702-021220/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9702-021220/211
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-9702-021220/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9702-021220/213
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9702-021220/214
Use of Hard-	24-Nov-20	7.5	An issue was discovered on	N/A	H-CDA-9702-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			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. **CVE ID : CVE-2020-29062**		021220/215
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9702-021220/216
97042p					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-9704-021220/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-9704-021220/218
Improper Neutralization of Special Elements	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-9704-021220/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9704-021220/220
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-9704-021220/221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9704-021220/222
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-9704-021220/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9704-021220/224
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9704-021220/225
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	H-CDA-9704-021220/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
97084p					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9708-021220/227
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	H-CDA-9708-021220/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9708-021220/229
N/A	24-Nov-20	7.8	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-9708-021220/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-9708-021220/231
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-9708-021220/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-9708-021220/233
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-9708-021220/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-9708-021220/235
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9708-021220/236
97168p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-9716-021220/237
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-9716-021220/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-9716-021220/239
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-9716-021220/240
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	H-CDA-9716-021220/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-9716-021220/242
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-9716-021220/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-9716-021220/244
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	H-CDA-9716-021220/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29062		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-9716-021220/246
fd1002s					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD10-021220/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD10-021220/248
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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.	N/A	H-CDA-FD10-021220/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29056		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD10-021220/250
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD10-021220/251
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-FD10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29059**		021220/252
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD10-021220/253
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD10-021220/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD10-021220/255
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	H-CDA-FD10-021220/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1104					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD11-021220/257
Cleartext Transmissio n of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-FD11-021220/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and conduct man-in-the-middle attacks on the management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD11-021220/259
N/A	24-Nov-20	7.8	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.	N/A	H-CDA-FD11-021220/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29057		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD11-021220/261
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD11-021220/262
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD11-021220/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD11-021220/264
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-FD11-021220/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD11-021220/266
fd1104b					
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-FD11-021220/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD11-021220/268
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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	N/A	H-CDA-FD11-021220/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD11-021220/270
Insufficiently Protected Credentials	24-Nov-20	5	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.	N/A	H-CDA-FD11-021220/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29058		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD11-021220/272
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD11-021220/273
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B,	N/A	H-CDA-FD11-021220/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD11-021220/275
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	H-CDA-FD11-021220/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(*&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1104s					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD11-021220/277
Cleartext Transmissio n of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-FD11-021220/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD11-021220/279
N/A	24-Nov-20	7.8	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	N/A	H-CDA-FD11-021220/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending random bytes to the telnet server on port 23, aka a "shawarma" attack. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD11-021220/281
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD11-021220/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD11-021220/283
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD11-021220/284
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD11-021220/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD11-021220/286
fd1104sn					
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	H-CDA-FD11-021220/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD11-021220/288
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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,	N/A	H-CDA-FD11-021220/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD11-021220/290
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-FD11-021220/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD11-021220/292
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD11-021220/293
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-FD11-021220/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD11-021220/295
Inadequate Encryption Strength	24-Nov-20	5	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,	N/A	H-CDA-FD11-021220/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1108s					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD11-021220/297
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-FD11-021220/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD11-021220/299
N/A	24-Nov-20	7.8	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,	N/A	H-CDA-FD11-021220/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD11-021220/301
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-FD11-021220/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD11-021220/303
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD11-021220/304
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD11-021220/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD11-021220/306
fd1204s-r2					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-FD12-021220/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD12-021220/308
Improper Neutralization of Special Elements used in a Command ('Command	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-FD12-021220/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD12-021220/310
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	H-CDA-FD12-021220/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD12-021220/312
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	H-CDA-FD12-021220/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29060		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD12-021220/314
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD12-021220/315
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-FD12-021220/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1204sn					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD12-021220/317
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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,	N/A	H-CDA-FD12-021220/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD12-021220/319
N/A	24-Nov-20	7.8	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,	N/A	H-CDA-FD12-021220/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD12-021220/321
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD12-021220/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD12-021220/323
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD12-021220/324
Use of Hard-	24-Nov-20	7.5	An issue was discovered on	N/A	H-CDA-FD12-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			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. **CVE ID : CVE-2020-29062**		021220/325
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD12-021220/326
fd1204sn-r2					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD12-021220/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD12-021220/328
Improper Neutralization of Special Elements	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD12-021220/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD12-021220/330
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-FD12-021220/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD12-021220/332
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-FD12-021220/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD12-021220/334
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD12-021220/335
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	H-CDA-FD12-021220/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1208s-r2					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD12-021220/337
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	H-CDA-FD12-021220/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD12-021220/339
N/A	24-Nov-20	7.8	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD12-021220/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD12-021220/341
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	H-CDA-FD12-021220/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD12-021220/343
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-FD12-021220/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD12-021220/345
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD12-021220/346
fd1216s-r1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD12-021220/347
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD12-021220/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD12-021220/349
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD12-021220/350
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	H-CDA-FD12-021220/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD12-021220/352
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD12-021220/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD12-021220/354
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	H-CDA-FD12-021220/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29062		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD12-021220/356
fd1608gs					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD16-021220/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD16-021220/358
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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.	N/A	H-CDA-FD16-021220/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29056		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD16-021220/360
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD16-021220/361
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-FD16-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29059**		021220/362
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD16-021220/363
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD16-021220/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD16-021220/365
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	H-CDA-FD16-021220/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1608sn					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD16-021220/367
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-FD16-021220/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and conduct man-in-the-middle attacks on the management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD16-021220/369
N/A	24-Nov-20	7.8	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.	N/A	H-CDA-FD16-021220/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29057		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD16-021220/371
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD16-021220/372
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	H-CDA-FD16-021220/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD16-021220/374
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	H-CDA-FD16-021220/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD16-021220/376
fd1616gs					
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-FD16-021220/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD16-021220/378
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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	N/A	H-CDA-FD16-021220/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD16-021220/380
Insufficiently Protected Credentials	24-Nov-20	5	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.	N/A	H-CDA-FD16-021220/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29058		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD16-021220/382
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD16-021220/383
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B,	N/A	H-CDA-FD16-021220/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD16-021220/385
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	H-CDA-FD16-021220/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1616sn					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	H-CDA-FD16-021220/387
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	H-CDA-FD16-021220/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	H-CDA-FD16-021220/389
N/A	24-Nov-20	7.8	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	N/A	H-CDA-FD16-021220/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending random bytes to the telnet server on port 23, aka a "shawarma" attack. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	H-CDA-FD16-021220/391
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD16-021220/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD16-021220/393
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	H-CDA-FD16-021220/394
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	H-CDA-FD16-021220/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	H-CDA-FD16-021220/396
fd8000					
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	H-CDA-FD80-021220/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	H-CDA-FD80-021220/398
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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,	N/A	H-CDA-FD80-021220/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	H-CDA-FD80-021220/400
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	H-CDA-FD80-021220/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	H-CDA-FD80-021220/402
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	H-CDA-FD80-021220/403
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	H-CDA-FD80-021220/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	H-CDA-FD80-021220/405
Inadequate Encryption Strength	24-Nov-20	5	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,	N/A	H-CDA-FD80-021220/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
Operating System					
cdata					
72408a_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-7240-021220/407
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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,	N/A	O-CDA-7240-021220/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-7240-021220/409
N/A	24-Nov-20	7.8	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,	N/A	O-CDA-7240-021220/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-7240-021220/411
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-7240-021220/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-7240-021220/413
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-7240-021220/414
Use of Hard-	24-Nov-20	7.5	An issue was discovered on	N/A	O-CDA-7240-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			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. **CVE ID : CVE-2020-29062**		021220/415
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-7240-021220/416
9008a_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-9008-021220/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9008-021220/418
Improper Neutralization of Special Elements	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-9008-021220/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9008-021220/420
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-9008-021220/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9008-021220/422
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-9008-021220/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9008-021220/424
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9008-021220/425
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-9008-021220/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
9016a_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9016-021220/427
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	O-CDA-9016-021220/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9016-021220/429
N/A	24-Nov-20	7.8	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-9016-021220/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9016-021220/431
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-9016-021220/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9016-021220/433
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-9016-021220/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9016-021220/435
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9016-021220/436
92408a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9240-021220/437
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9240-021220/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9240-021220/439
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9240-021220/440
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-9240-021220/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9240-021220/442
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-9240-021220/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9240-021220/444
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	O-CDA-9240-021220/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29062		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9240-021220/446
92416a_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9241-021220/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9241-021220/448
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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.	N/A	O-CDA-9241-021220/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29056		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9241-021220/450
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9241-021220/451
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	O-CDA-9241-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29059**		021220/452
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9241-021220/453
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-9241-021220/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9241-021220/455
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	O-CDA-9241-021220/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
9288_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9288-021220/457
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-9288-021220/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and conduct man-in-the-middle attacks on the management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9288-021220/459
N/A	24-Nov-20	7.8	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.	N/A	O-CDA-9288-021220/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29057		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9288-021220/461
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9288-021220/462
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-9288-021220/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9288-021220/464
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-9288-021220/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9288-021220/466
97016_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	O-CDA-9701-021220/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9701-021220/468
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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	N/A	O-CDA-9701-021220/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9701-021220/470
Insufficiently Protected Credentials	24-Nov-20	5	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.	N/A	O-CDA-9701-021220/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29058		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9701-021220/472
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9701-021220/473
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B,	N/A	O-CDA-9701-021220/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9701-021220/475
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	O-CDA-9701-021220/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
97024p_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9702-021220/477
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-9702-021220/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9702-021220/479
N/A	24-Nov-20	7.8	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	N/A	O-CDA-9702-021220/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending random bytes to the telnet server on port 23, aka a "shawarma" attack. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9702-021220/481
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9702-021220/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9702-021220/483
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9702-021220/484
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-9702-021220/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9702-021220/486
97028p_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	O-CDA-9702-021220/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9702-021220/488
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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,	N/A	O-CDA-9702-021220/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9702-021220/490
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	O-CDA-9702-021220/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9702-021220/492
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9702-021220/493
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	O-CDA-9702-021220/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9702-021220/495
Inadequate Encryption Strength	24-Nov-20	5	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,	N/A	O-CDA-9702-021220/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
97042p_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9704-021220/497
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-9704-021220/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9704-021220/499
N/A	24-Nov-20	7.8	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,	N/A	O-CDA-9704-021220/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9704-021220/501
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-9704-021220/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9704-021220/503
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9704-021220/504
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-9704-021220/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9704-021220/506
97084p_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-9708-021220/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-9708-021220/508
Improper Neutralization of Special Elements used in a Command ('Command	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-9708-021220/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-9708-021220/510
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	O-CDA-9708-021220/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-9708-021220/512
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	O-CDA-9708-021220/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29060		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9708-021220/514
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-9708-021220/515
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-9708-021220/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
97168p_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-9716-021220/517
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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,	N/A	O-CDA-9716-021220/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-9716-021220/519
N/A	24-Nov-20	7.8	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,	N/A	O-CDA-9716-021220/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-9716-021220/521
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-9716-021220/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-9716-021220/523
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-9716-021220/524
Use of Hard-	24-Nov-20	7.5	An issue was discovered on	N/A	O-CDA-9716-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			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. **CVE ID : CVE-2020-29062**		021220/525
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-9716-021220/526
fd1002s_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD10-021220/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD10-021220/528
Improper Neutralization of Special Elements	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD10-021220/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD10-021220/530
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD10-021220/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD10-021220/532
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD10-021220/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD10-021220/534
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD10-021220/535
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-FD10-021220/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1104_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD11-021220/537
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	O-CDA-FD11-021220/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD11-021220/539
N/A	24-Nov-20	7.8	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD11-021220/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD11-021220/541
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD11-021220/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD11-021220/543
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD11-021220/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD11-021220/545
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD11-021220/546
fd1104b_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD11-021220/547
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD11-021220/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD11-021220/549
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD11-021220/550
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-FD11-021220/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD11-021220/552
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD11-021220/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD11-021220/554
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	O-CDA-FD11-021220/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29062		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD11-021220/556
fd1104s_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD11-021220/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD11-021220/558
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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.	N/A	O-CDA-FD11-021220/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29056		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD11-021220/560
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD11-021220/561
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	O-CDA-FD11-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29059**		021220/562
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD11-021220/563
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD11-021220/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD11-021220/565
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	O-CDA-FD11-021220/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1104sn_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD11-021220/567
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-FD11-021220/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and conduct man-in-the-middle attacks on the management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD11-021220/569
N/A	24-Nov-20	7.8	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.	N/A	O-CDA-FD11-021220/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29057		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD11-021220/571
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD11-021220/572
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD11-021220/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD11-021220/574
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD11-021220/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD11-021220/576
fd1108s_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	O-CDA-FD11-021220/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD11-021220/578
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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	N/A	O-CDA-FD11-021220/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD11-021220/580
Insufficiently Protected Credentials	24-Nov-20	5	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.	N/A	O-CDA-FD11-021220/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29058		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD11-021220/582
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD11-021220/583
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B,	N/A	O-CDA-FD11-021220/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD11-021220/585
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	O-CDA-FD11-021220/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			store encrypted passwords. This algorithm will XOR the password with the hardcoded *j7a(L#yZ98sSd5HfSgGjMj8;Ss;d)(*&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd1204s-r2_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD12-021220/587
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-FD12-021220/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD12-021220/589
N/A	24-Nov-20	7.8	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	N/A	O-CDA-FD12-021220/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending random bytes to the telnet server on port 23, aka a "shawarma" attack. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD12-021220/591
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD12-021220/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD12-021220/593
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD12-021220/594
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD12-021220/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD12-021220/596
fd1204sn_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	O-CDA-FD12-021220/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. Attackers can use "show system infor" to discover cleartext TELNET credentials. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD12-021220/598
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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,	N/A	O-CDA-FD12-021220/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. One can escape from a shell and acquire root privileges by leveraging the TFTP download configuration. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD12-021220/600
Insufficiently Protected Credentials	24-Nov-20	5	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	N/A	O-CDA-FD12-021220/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD12-021220/602
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD12-021220/603
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	O-CDA-FD12-021220/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD12-021220/605
Inadequate Encryption Strength	24-Nov-20	5	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,	N/A	O-CDA-FD12-021220/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1204sn-r2_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD12-021220/607
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-FD12-021220/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD12-021220/609
N/A	24-Nov-20	7.8	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,	N/A	O-CDA-FD12-021220/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD12-021220/611
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD12-021220/612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD12-021220/613
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD12-021220/614
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD12-021220/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD12-021220/616
fd1208s-r2_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD12-021220/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD12-021220/618
Improper Neutralization of Special Elements used in a Command ('Command	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD12-021220/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD12-021220/620
Insufficiently Protected Credentials	24-Nov-20	5	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,	N/A	O-CDA-FD12-021220/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. Attackers can discover cleartext web-server credentials via certain /opt/lighttpd/web/cgi/ requests. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD12-021220/622
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	O-CDA-FD12-021220/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29060		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD12-021220/624
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD12-021220/625
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD12-021220/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1216s-r1_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD12-021220/627
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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,	N/A	O-CDA-FD12-021220/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD12-021220/629
N/A	24-Nov-20	7.8	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,	N/A	O-CDA-FD12-021220/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD12-021220/631
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD12-021220/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1616GS, FD1616SN, and FD8000 devices. There is a default panger123 password for the suma123 account for certain old firmware. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD12-021220/633
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD12-021220/634
Use of Hard-	24-Nov-20	7.5	An issue was discovered on	N/A	O-CDA-FD12-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			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. **CVE ID : CVE-2020-29062**		021220/635
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD12-021220/636
fd1608gs_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD16-021220/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29054**		
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD16-021220/638
Improper Neutralization of Special Elements	24-Nov-20	10	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD16-021220/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			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. **CVE ID : CVE-2020-29056**		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD16-021220/640
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD16-021220/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD16-021220/642
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD16-021220/643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD16-021220/644
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD16-021220/645
Inadequate Encryption Strength	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-FD16-021220/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29063**		
fd1608sn_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD16-021220/647
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P,	N/A	O-CDA-FD16-021220/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD16-021220/649
N/A	24-Nov-20	7.8	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD16-021220/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29057**		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD16-021220/651
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P, 97042P, 97084P, 97168P, FD1002S, FD1104, FD1104B, FD1104S, FD1104SN,	N/A	O-CDA-FD16-021220/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29059**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD16-021220/653
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD16-021220/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD16-021220/655
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD16-021220/656
fd1616gs_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD16-021220/657
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD16-021220/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD16-021220/659
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD16-021220/660
Insufficiently Protected Credentials	24-Nov-20	5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288,	N/A	O-CDA-FD16-021220/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29058**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD16-021220/662
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD16-021220/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1204SN, FD1204SN-R2, FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default debug124 password for the debug account. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD16-021220/664
Use of Hard-coded Credentials	24-Nov-20	7.5	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.	N/A	O-CDA-FD16-021220/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29062		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD16-021220/666
fd1616sn_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD16-021220/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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. **CVE ID : CVE-2020-29055**	N/A	O-CDA-FD16-021220/668
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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.	N/A	O-CDA-FD16-021220/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29056		
N/A	24-Nov-20	7.8	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. **CVE ID : CVE-2020-29057**	N/A	O-CDA-FD16-021220/670
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD16-021220/671
Use of Hard-coded	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A,	N/A	O-CDA-FD16-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			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. **CVE ID : CVE-2020-29059**		021220/672
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29060**	N/A	O-CDA-FD16-021220/673
Use of Hard-coded Credentials	24-Nov-20	7.5	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,	N/A	O-CDA-FD16-021220/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD1208S-R2, FD1216S-R1, FD1608GS, FD1608SN, FD1616GS, FD1616SN, and FD8000 devices. There is a default root126 password for the root account. **CVE ID : CVE-2020-29061**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29062**	N/A	O-CDA-FD16-021220/675
Inadequate Encryption Strength	24-Nov-20	5	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	N/A	O-CDA-FD16-021220/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			j7a(L#yZ98sSd5HfSgGjMj8;Ss ;d)(&^#@$a2s0i3g value. **CVE ID : CVE-2020-29063**		
fd8000_firmware					
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29054**	N/A	O-CDA-FD80-021220/677
Cleartext Transmission of Sensitive Information	24-Nov-20	4.3	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	N/A	O-CDA-FD80-021220/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and conduct man-in-the-middle attacks on the management of the appliance. **CVE ID : CVE-2020-29055**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Nov-20	10	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. **CVE ID : CVE-2020-29056**	N/A	O-CDA-FD80-021220/679
N/A	24-Nov-20	7.8	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.	N/A	O-CDA-FD80-021220/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-29057		
Insufficiently Protected Credentials	24-Nov-20	5	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. **CVE ID : CVE-2020-29058**	N/A	O-CDA-FD80-021220/681
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29059**	N/A	O-CDA-FD80-021220/682
Use of Hard-coded Credentials	24-Nov-20	7.5	An issue was discovered on CDATA 72408A, 9008A, 9016A, 92408A, 92416A, 9288, 97016, 97024P, 97028P,	N/A	O-CDA-FD80-021220/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-29060**		
Use of Hard-coded Credentials	24-Nov-20	7.5	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. **CVE ID : CVE-2020-29061**	N/A	O-CDA-FD80-021220/684
Use of Hard-coded Credentials	24-Nov-20	7.5	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	N/A	O-CDA-FD80-021220/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FD8000 devices. There is a default blank password for the guest account. **CVE ID : CVE-2020-29062**		
Inadequate Encryption Strength	24-Nov-20	5	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. **CVE ID : CVE-2020-29063**	N/A	O-CDA-FD80-021220/686
Debian					
debian_linux					
Argument Injection or Modification	18-Nov-20	5.1	Go before 1.14.12 and 1.15.x before 1.15.5 allows Argument Injection. **CVE ID : CVE-2020-28367**	https://groups.google.com/g/golang-announce/c/NpBGTTmKzpM	O-DEB-DEBI-021220/687
Fedoraproject					
fedora					
Improper Control of Generation	18-Nov-20	5.1	Go before 1.14.12 and 1.15.x before 1.15.5 allows Code Injection.	https://groups.google.com/g/g	O-FED-FEDO-021220/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			**CVE ID : CVE-2020-28366**	olang-announce/c/NpBGTTmKzpM	
Argument Injection or Modification	18-Nov-20	5.1	Go before 1.14.12 and 1.15.x before 1.15.5 allows Argument Injection. **CVE ID : CVE-2020-28367**	https://groups.google.com/g/golang-announce/c/NpBGTTmKzpM	O-FED-FEDO-021220/689
Uncontrolled Resource Consumption	19-Nov-20	5	A Node.js application that allows an attacker to trigger a DNS request for a host of their choice could trigger a Denial of Service in versions < 15.2.1, < 14.15.1, and < 12.19.1 by getting the application to resolve a DNS record with a larger number of responses. This is fixed in 15.2.1, 14.15.1, and 12.19.1. **CVE ID : CVE-2020-8277**	https://nodejs.org/en/blog/vulnerability/november-2020-security-releases/	O-FED-FEDO-021220/690
HP					
hp-ux					
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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. **CVE ID : CVE-2020-4937**	https://www.ibm.com/support/pages/node/6370795	O-HP-HP-U-021220/691
IBM					
AIX					
Improper Authenticati	23-Nov-20	5	IBM Spectrum Protect Operations Center 8.1.0.000	https://www.ibm.co	O-IBM-AIX-021220/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			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. **CVE ID : CVE-2020-4771**	m/support/pages/node/6369101	
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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. **CVE ID : CVE-2020-4937**	https://www.ibm.com/support/pages/node/6370795	O-IBM-AIX-021220/693
i					
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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. **CVE ID : CVE-2020-4937**	https://www.ibm.com/support/pages/node/6370795	O-IBM-I-021220/694
Linux					
linux_kernel					
Improper Authentication	23-Nov-20	5	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	https://www.ibm.com/support/pages/no	O-LIN-LINU-021220/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-4771**	de/6369101	
Information Exposure	23-Nov-20	4.3	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. **CVE ID : CVE-2020-4783**	https://www.ibm.com/support/pages/node/6368601	O-LIN-LINU-021220/696
Use of Hard-coded Credentials	23-Nov-20	7.5	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. **CVE ID : CVE-2020-4854**	https://www.ibm.com/support/pages/node/6367823	O-LIN-LINU-021220/697
Use of a Broken or Risky	20-Nov-20	5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.2 uses weaker	https://www.ibm.com/support	O-LIN-LINU-021220/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 191814. **CVE ID : CVE-2020-4937**	/pages/node/6370795	
Microsoft					
windows					
Unquoted Search Path or Element	19-Nov-20	4.4	A CWE-428 Windows Unquoted Search Path vulnerability exists in EcoStruxure Building Operation Enterprise Server installer V1.9 - V3.1 and Enterprise Central installer V2.0 - V3.1 that could cause any local Windows user who has write permission on at least one of the subfolders of the Connect Agent service binary path, being able to gain the privilege of the user who started the service. By default, the Enterprise Server and Enterprise Central is always installed at a location requiring Administrator privileges so the vulnerability is only valid if the application has been installed on a non-secure location. **CVE ID : CVE-2020-28209**	N/A	O-MIC-WIND-021220/699
Improper Authentication	23-Nov-20	5	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	https://www.ibm.com/support/pages/node/6369101	O-MIC-WIND-021220/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2020-4771**		
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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. **CVE ID : CVE-2020-4937**	https://www.ibm.com/support/pages/node/6370795	O-MIC-WIND-021220/701
Oracle					
solaris					
Use of a Broken or Risky Cryptographic Algorithm	20-Nov-20	5	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. **CVE ID : CVE-2020-4937**	https://www.ibm.com/support/pages/node/6370795	O-ORA-SOLA-021220/702