# BULLETIN (SB20-272)
# VULNERABILITY SUMMARY FOR THE WEEK OF
# 21ST SEPTEMBER, 2020

# Bulletin (SB20-272)
# Vulnerability Summary for the Week of September 21, 2020

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

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

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

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| aveva -- edna_enterprise_data_historian | An SQL injection vulnerability exists in the Alias.asmx Web Service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Parameter AliasName in Alias.asmx is vulnerable to unauthenticated SQL injection attacks. An attacker can send unauthenticated HTTP requests to trigger this vulnerability. | 2020-09-24 | 7.5 | CVE-2020-13508 MISC |
| aveva -- edna_enterprise_data_historian | Parameter psClass in ednareporting.asmx is vulnerable to unauthenticated SQL injection attacks. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. An attacker can send unauthenticated HTTP requests to trigger this vulnerability. | 2020-09-24 | 7.5 | CVE-2020-13505 MISC |
| aveva -- edna_enterprise_data_historian | Parameter AttFilterName in ednareporting.asmx is vulnerable to unauthenticated SQL injection attacks. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. An attacker can send unauthenticated HTTP requests to trigger this vulnerability. | 2020-09-24 | 7.5 | CVE-2020-13503 MISC |
| aveva -- edna_enterprise_data_historian | An SQL injection vulnerability exists in the CHaD.asmx web service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. Parameter InstanceName in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks. | 2020-09-24 | 7.5 | CVE-2020-13501 MISC |
| aveva -- edna_enterprise_data_historian | SQL injection vulnerability exists in the CHaD.asmx web service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. Parameter ClassName in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks. | 2020-09-24 | 7.5 | CVE-2020-13500 MISC |
| aveva -- edna_enterprise_data_historian | An SQL injection vulnerability exists in the CHaD.asmx web service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Specially crafted SOAP web requests can cause SQL injections resulting in data compromise. Parameter InstancePath in CHaD.asmx is vulnerable to unauthenticated SQL injection attacks. | 2020-09-24 | 7.5 | CVE-2020-13499 MISC |
| aveva -- edna_enterprise_data_historian | An SQL injection vulnerability exists in the Alias.asmx Web Service functionality of eDNA Enterprise Data Historian 3.0.1.2/7.5.4989.33053. Parameter OrigID in Alias.asmx is vulnerable to unauthenticated SQL injection attacks An attacker can send unauthenticated HTTP requests to trigger this vulnerability. | 2020-09-24 | 7.5 | CVE-2020-13507 MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/mailAdmin.php. | 2020-09-24 | 7.5 | CVE-2020-12838 MISC MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to malicious file uploads via the form for uploading sounds to garage doors. The magic bytes for WAV must be used. | 2020-09-24 | 7.5 | CVE-2020-12843 MISC MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/checkUserExpirationDate.php. | 2020-09-24 | 7.5 | CVE-2020-12842 MISC MISC |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to privilege escalation by appending PHP code to /cron/checkExpirationDate.php. | 2020-09-24 | 7.5 | CVE-2020-12839 MISC MISC |
| google -- android | In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-143604331 | 2020-09-18 | 7.5 | CVE-2020-0354 MISC |
| google -- chrome | Use after free in WebXR in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6551 MISC MISC FEDORA |
| google -- chrome | Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6549 MISC MISC FEDORA |
| google -- chrome | Use after free in IndexedDB in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6550 MISC MISC FEDORA |
| google -- chrome | Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6548 MISC MISC FEDORA |
| google -- chrome | Use after free in Blink in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6552 MISC MISC FEDORA |
| google -- chrome | Use after free in offline mode in Google Chrome on iOS prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6553 MISC MISC FEDORA |
| google -- chrome | Heap buffer overflow in SwiftShader in Google Chrome prior to 84.0.4147.135 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 9.3 | CVE-2020-6556 MISC MISC FEDORA |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could allow a remote authenticated attacker to upload arbitrary files, caused by the improper validation of file extensions. By sending a specially-crafted HTTP request, a remote attacker could exploit this vulnerability to upload a malicious file, which could allow the attacker to execute arbitrary code on the vulnerable system. IBM X-Force ID: 184979. | 2020-09-22 | 9 | CVE-2020-4620 XF CONFIRM |
| ozeki -- ozeki_ng_sms_gateway | An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The outbox functionality of the TXT File module can be used to delete all/most files in a folder. Because the product usually runs as NT AUTHORITY\SYSTEM, the only files that will not be deleted are those currently being run by the system and/or files that have special security attributes (e.g., Windows Defender files). | 2020-09-22 | 9 | CVE-2020-14031 MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. By leveraging a path traversal vulnerability in the Autoreply module's Script Name, an attacker may write to or overwrite arbitrary files, with arbitrary content, usually with NT AUTHORITY\SYSTEM privileges. | 2020-09-22 | 9 | CVE-2020-14028 MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | Ozeki NG SMS Gateway 4.17.1 through 4.17.6 does not check the file type when bulk importing new contacts ("Import Contacts" functionality) from a file. It is possible to upload an executable or .bat file that can be executed with the help of a functionality (E.g. the "Application Starter" module) within the application. | 2020-09-22 | 9 | CVE-2020-14022 MISC MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | CSV Injection (aka Excel Macro Injection or Formula Injection) exists in the Export Of Contacts feature in Ozeki NG SMS Gateway through 4.17.6 via a value that is mishandled in a CSV export. | 2020-09-22 | 9.3 | CVE-2020-14026 MISC MISC MISC |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| adobe -- media_encoder | Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. | 2020-09-18 | 5.8 | CVE-2020-9745 MISC |
| adobe -- media_encoder | Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. | 2020-09-18 | 5.8 | CVE-2020-9744 MISC |
| adobe -- media_encoder | Adobe Media Encoder version 14.3.2 (and earlier versions) has an out-of-bounds read vulnerability that could be exploited to read past the end of an allocated buffer, possibly resulting in a crash or disclosure of sensitive information from other memory locations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. | 2020-09-18 | 5.8 | CVE-2020-9739 MISC |
| buffalo -- airstation_whr-g54s_firmware | Directory traversal vulnerability in WHR-G54S firmware 1.43 and earlier allows an attacker to access sensitive information such as setting values via unspecified vectors. | 2020-09-18 | 4 | CVE-2020-5605 MISC MISC |
| buffalo -- airstation_whr-g54s_firmware | Cross-site scripting vulnerability in WHR-G54S firmware 1.43 and earlier allows remote attackers to inject arbitrary script via a specially crafted page. | 2020-09-18 | 4.3 | CVE-2020-5606 MISC MISC |
| corephp -- pago_commerce | The paGO Commerce plugin 2.5.9.0 for Joomla! allows SQL Injection via the administrator/index.php?option=com_pago&view=comments filter_published parameter. | 2020-09-18 | 6.5 | CVE-2020-25751 MISC MISC |
| cpanel -- cpanel | cPanel before 90.0.10 allows self XSS via the Cron Editor interface (SEC-574). | 2020-09-25 | 4.3 | CVE-2020-26115 MISC |
| cpanel -- cpanel | cPanel before 90.0.10 allows self XSS via the Cron Jobs interface (SEC-573). | 2020-09-25 | 4.3 | CVE-2020-26114 MISC |
| gogogate -- ismartgate_pro_firmware | iSmartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to open/close a specified garage door/gate via /isg/opendoor.php. | 2020-09-24 | 4.3 | CVE-2020-12280 MISC MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to malicious file uploads via the form for uploading images to garage doors. The magic bytes of PNG must be used. | 2020-09-24 | 5 | CVE-2020-12837 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | | | | MISC<br>MISC |
| gogogate -- ismartgate_pro_firmware | iSmartgate PRO 1.5.9 is vulnerable to CSRF via the busca parameter in the form used for searching for users, accessible via /index.php. (This can be combined with reflected XSS.) | 2020-09-24 | 6.8 | CVE-2020-12282<br>MISC<br>MISC |
| gogogate -- ismartgate_pro_firmware | iSmartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to create a new user via /index.php. | 2020-09-24 | 4.3 | CVE-2020-12281<br>MISC<br>MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to upload sound files via /index.php | 2020-09-24 | 4.3 | CVE-2020-12840<br>MISC<br>MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to CSRF that allows remote attackers to upload imae files via /index.php | 2020-09-24 | 4.3 | CVE-2020-12841<br>MISC<br>MISC |
| gogogate -- ismartgate_pro_firmware | ismartgate PRO 1.5.9 is vulnerable to clickjacking. | 2020-09-24 | 4.3 | CVE-2020-13119<br>MISC<br>MISC |
| google -- android | In iptables, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-136658008 | 2020-09-18 | 4.6 | CVE-2020-0347<br>MISC |
| google -- android | In NFC, there is a possible out of bounds read due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148736216 | 2020-09-18 | 5 | CVE-2020-0300<br>MISC |
| google -- android | In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137868765 | 2020-09-18 | 6.8 | CVE-2020-0319<br>MISC |
| google -- android | In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139424089 | 2020-09-18 | 4.6 | CVE-2020-0350<br>MISC |
| google -- android | In the Settings app, there is an insecure default value. This could lead to local escalation of privilege and tapjacking with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144507081 | 2020-09-18 | 4.4 | CVE-2020-0271<br>MISC |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In NFC, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-148294643 | 2020-09-18 | 4.4 | CVE-2020-0268 MISC |
| google -- android | In NetworkStackNotifier, there is a possible permissions bypass due to an unsafe implicit PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157475111 | 2020-09-18 | 4.6 | CVE-2020-0405 MISC |
| google -- android | In Bluetooth, there is a possible spoofing of bluetooth device metadata due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145130119 | 2020-09-18 | 4.6 | CVE-2020-0299 MISC |
| google -- android | In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147995915 | 2020-09-18 | 4.6 | CVE-2020-0334 MISC |
| google -- android | In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over NFC with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139188582 | 2020-09-18 | 4 | CVE-2020-0348 MISC |
| google -- android | In Bluetooth, there is a possible control over Bluetooth enabled state due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145129266 | 2020-09-18 | 4.6 | CVE-2020-0298 MISC |
| google -- android | In NFC, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-122361504 | 2020-09-18 | 4.6 | CVE-2020-0335 MISC |
| google -- android | In WiFi tethering, there is a possible attacker controlled intent due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156353008 | 2020-09-18 | 4.6 | CVE-2020-0262 MISC |
| google -- android | In the audio server, there is a missing permission check. This could lead to local escalation of privilege regarding audio settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137015603 | 2020-09-18 | 4.6 | CVE-2020-0089 MISC |
| google -- android | In the System UI, there is a possible system crash due to an uncaught exception. This could lead to local permanent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-33646131 | 2020-09-18 | 4.9 | CVE-2020-0318 MISC |
| google -- android | In the Bluetooth server, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System privileges and a Firmware compromise needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147227320 | 2020-09-18 | 4.6 | CVE-2020-0309 MISC |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Out of bounds read in WebGL in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. | 2020-09-21 | 4.3 | CVE-2020-6555 MISC MISC FEDORA |
| google -- chrome | Insufficient data validation in Omnibox in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. | 2020-09-21 | 4.3 | CVE-2020-6571 SUSE SUSE SUSE MISC MISC FEDORA |
| google -- chrome | Information leakage in WebRTC in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information via a crafted WebRTC interaction. | 2020-09-21 | 4.3 | CVE-2020-6570 SUSE SUSE SUSE MISC MISC FEDORA |
| google -- chrome | Insufficient policy enforcement in Blink in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page. | 2020-09-21 | 4.3 | CVE-2020-6562 SUSE SUSE SUSE MISC MISC FEDORA |
| google -- chrome | Insufficient policy enforcement in iOSWeb in Google Chrome on iOS prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. | 2020-09-21 | 4.3 | CVE-2020-6558 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Insufficient policy validation in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. | 2020-09-21 | 6.8 | CVE-2020-15961 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Inappropriate implementation in WebView in Google Chrome on Android prior to 84.0.4147.105 allowed a remote attacker to leak cross-origin data via a crafted HTML page. | 2020-09-21 | 4.3 | CVE-2020-6538 MISC MISC FEDORA |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Heap buffer overflow in storage in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-15960 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension. | 2020-09-21 | 4.3 | CVE-2020-15966 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Insufficient policy enforcement in networking in Google Chrome prior to 85.0.4183.102 allowed an attacker who convinced the user to enable logging to obtain potentially sensitive information from process memory via social engineering. | 2020-09-21 | 4.3 | CVE-2020-15959 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6544 MISC MISC FEDORA |
| google -- chrome | Use after free in task scheduling in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6543 MISC MISC FEDORA |
| google -- chrome | Incorrect security UI in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially obtain sensitive information via a crafted HTML page. | 2020-09-21 | 4.3 | CVE-2020-6547 MISC MISC FEDORA |
| google -- chrome | Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. | 2020-09-21 | 6.8 | CVE-2020-15963 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Use after free in WebUSB in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6541 MISC MISC FEDORA |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Insufficient policy validation in serial in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-15962 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Use after free in audio in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6545 MISC MISC FEDORA |
| google -- chrome | Use after free in extensions in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension. | 2020-09-21 | 6.8 | CVE-2020-6554 MISC MISC FEDORA |
| google -- chrome | Use after free in video in Google Chrome on Android prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6573 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Use after free in ANGLE in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6542 MISC MISC FEDORA |
| google -- chrome | Insufficient data validation in media in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-15964 SUSE SUSE SUSE MISC MISC |
| google -- chrome | Buffer overflow in Skia in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6540 MISC MISC FEDORA |
| google -- chrome | Inappropriate implementation in installer in Google Chrome prior to 84.0.4147.125 allowed a local attacker to potentially elevate privilege via a crafted filesystem. | 2020-09-21 | 4.6 | CVE-2020-6546 MISC MISC FEDORA |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Use after free in CSS in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6539 MISC MISC FEDORA |
| google -- chrome | Type confusion in V8 in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6537 MISC MISC FEDORA |
| google -- chrome | Use after free in SCTP in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-6532 MISC MISC FEDORA |
| google -- chrome | Type confusion in V8 in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. | 2020-09-21 | 6.8 | CVE-2020-15965 SUSE SUSE SUSE MISC MISC |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2017.1 - 2020.2.4. Unrestricted access to a high-level system-usage summary allows an attacker to obtain project names and usage metrics. | 2020-09-18 | 5 | CVE-2020-15775 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2018.2 and Gradle Enterprise Build Cache Node 4.1. CSRF mitigation can be bypassed because cross-site transmission of a cookie (containing a CSRF token) can occur. | 2020-09-18 | 5 | CVE-2020-15771 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2017.3 - 2020.2.4 and Gradle Enterprise Build Cache Node 1.0 - 9.2. Unrestricted HTTP header reflection allows remote attackers to obtain authentication cookies (if an XSS issue exists) via the /info/headers, /cache-info/headers, /admin-info/headers, /distribution-broker-info/headers, or /cache-node-info/headers path. | 2020-09-18 | 5 | CVE-2020-15768 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2018.5. There is a lack of lock-out after excessive failed login attempts. This allows a remote attacker to conduct brute-force guessing of a local user's password. | 2020-09-18 | 5 | CVE-2020-15770 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2020.2 - 2020.2.4. An XSS issue exists via the request URL. | 2020-09-18 | 4.3 | CVE-2020-15769 MISC CONFIRM |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2018.5 - 2020.2.4. Because of implicitly remembered user-login information, physically proximate attackers can use a user session after browser closure. | 2020-09-18 | 4.6 | CVE-2020-15774 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise before 2020.2.4. Because of unrestricted cross-origin requests to read-only data in the Export API, an attacker can access data as a user (for the duration of the browser session) after previously explicitly authenticating with the API. | 2020-09-18 | 4 | CVE-2020-15773 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2018.5 - 2020.2.4. There is XXE with resultant SSRF via an uploaded SAML IDP configuration. | 2020-09-18 | 4 | CVE-2020-15772 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise 2018.2 - 2020.2.4. CSRF mitigation can be bypassed because the anti-CSRF token is in a cleartext cookie. | 2020-09-18 | 6.8 | CVE-2020-15776 MISC CONFIRM |
| gradle -- enterprise | An issue was discovered in Gradle Enterprise before 2020.2.5. Lack of the secure attribute on the anti-CSRF cookie allows an attacker (with the ability to read HTTP traffic) to obtain a user's anti-CSRF token if the user initiates a cleartext HTTP request. | 2020-09-18 | 4.3 | CVE-2020-15767 MISC CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 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: 184983. | 2020-09-22 | 5 | CVE-2020-4622 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could disclose sensitive username information to an attacker using a specially crafted HTTP request. IBM X-Force ID: 184929. | 2020-09-22 | 5 | CVE-2020-4616 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 184930. | 2020-09-22 | 5.8 | CVE-2020-4617 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt sensitive information. IBM X-Force ID: 184927. | 2020-09-22 | 5 | CVE-2020-4614 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 184925. | 2020-09-22 | 5 | CVE-2020-4613 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to obtain sensitive information using a specially crafted HTTP request. IBM X-Force ID: 184924. | 2020-09-22 | 4 | CVE-2020-4612 XF CONFIRM |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could allow a privileged user to cause a denial of service due to improper input validation. IBM X-Force ID: 184937. | 2020-09-22 | 4 | CVE-2020-4618 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 stores user credentials in plain in clear text which can be read by an authenticated user. IBM X-Force ID: 184976. | 2020-09-22 | 4 | CVE-2020-4619 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to escalate their privileges to administrator due to insufficient authorization checks. IBM X-Force ID: 184981. | 2020-09-22 | 6.5 | CVE-2020-4621 XF CONFIRM |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 could allow an authenticated user to bypass security and execute actions reserved for admins. IBM X-Force ID: 184922. | 2020-09-22 | 6.5 | CVE-2020-4611 XF CONFIRM |
| ibm -- datapower_gateway | IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a specially crafted a JSON request with invalid characters. IBM X-Force ID: 184439. | 2020-09-21 | 5 | CVE-2020-4580 XF CONFIRM |
| ibm -- datapower_gateway | IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a specially crafted HTTP/2 request with invalid characters. IBM X-Force ID: 184438. | 2020-09-21 | 5 | CVE-2020-4579 XF CONFIRM |
| ibm -- datapower_gateway | IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.12 could allow a remote attacker to cause a denial of service by sending a chunked transfer-encoding HTTP/2 request. IBM X-Force ID: 184441. | 2020-09-21 | 5 | CVE-2020-4581 XF CONFIRM |
| ibm -- websphere_application_server | IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information. IBM X-Force ID: 185590. | 2020-09-21 | 5 | CVE-2020-4643 XF CONFIRM |
| misp -- misp | An issue was discovered in MISP before 2.4.132. It can perform an unwanted action because of a POST operation on a form that is not linked to the login page. | 2020-09-18 | 5 | CVE-2020-25766 MISC MISC |
| nvidia -- geforce_now | NVIDIA GeForce NOW, versions prior to 2.0.23 (Windows, macOS) and versions prior to 5.31 (Android, Shield TV), contains a vulnerability in the application software where the network test component transmits sensitive information insecurely, which may lead to information disclosure. | 2020-09-18 | 5 | CVE-2020-5976 CONFIRM |
| nvidia -- geforce_now | NVIDIA GeForce NOW, versions prior to 2.0.23 on Windows and macOS, contains a vulnerability in the desktop application software that includes sensitive information as part of a URL, which may lead to information disclosure. | 2020-09-18 | 5 | CVE-2020-5975 CONFIRM |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ozeki -- ozeki_ng_sms_gateway | Ozeki NG SMS Gateway through 4.17.6 has multiple CSRF vulnerabilities. For example, an administrator, by following a link, can be tricked into making unwanted changes such as installing new modules or changing a password. | 2020-09-22 | 6.8 | CVE-2020-14025 MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The ASP.net SMS module can be used to read and validate the source code of ASP files. By altering the path, it can be made to read any file on the Operating System, usually with NT AUTHORITY\SYSTEM privileges. | 2020-09-18 | 4 | CVE-2020-14021 MISC MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | Ozeki NG SMS Gateway through 4.17.6 allows SSRF via SMS WCF or RSS To SMS. | 2020-09-22 | 4 | CVE-2020-14023 MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The RSS To SMS module processes XML files in an unsafe manner. This opens the application to an XML External Entity attack that can be used to perform SSRF or read arbitrary local files. | 2020-09-18 | 5 | CVE-2020-14029 MISC MISC |
| ozeki -- ozeki_ng_sms_gateway | Ozeki NG SMS Gateway through 4.17.6 has multiple authenticated stored and/or reflected XSS vulnerabilities via the (1) Receiver or Recipient field in the Mailbox feature, (2) OZFORM_GROUPNAME field in the Group configuration of addresses, (3) listname field in the Defining address lists configuration, or (4) any GET Parameter in the /default URL of the application. | 2020-09-22 | 4.3 | CVE-2020-14024 MISC MISC |
| philips -- clinical_collaboration_platform | Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties required to process the data safely and correctly. | 2020-09-18 | 4.3 | CVE-2020-14506 MISC |
| philips -- clinical_collaboration_platform | Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. When an attacker claims to have a given identity, the software does not prove or insufficiently proves the claim is correct. | 2020-09-18 | 5.8 | CVE-2020-16198 MISC |
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with From<InlineArray<A, T>>. | 2020-09-19 | 5 | CVE-2020-25793 MISC MISC |
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with pair(). | 2020-09-19 | 5 | CVE-2020-25792 MISC MISC |
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, the array size is not checked when constructed with unit(). | 2020-09-19 | 5 | CVE-2020-25791 MISC MISC |
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, insert_from can have a memory-safety issue upon a panic. | 2020-09-19 | 5 | CVE-2020-25795 MISC MISC |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the InlineArray implementation, an unaligned reference may be generated for a type that has a large alignment requirement. | 2020-09-19 | 5 | CVE-2020-25796 MISC MISC |
| rust-lang -- rust | An issue was discovered in the sized-chunks crate through 0.6.2 for Rust. In the Chunk implementation, clone can have a memory-safety issue upon a panic. | 2020-09-19 | 5 | CVE-2020-25794 MISC MISC |
| safervpn -- safervpn | SaferVPN before 5.0.3.3 on Windows could allow low-privileged users to create or overwrite arbitrary files, which could cause a denial of service (DoS) condition, because a symlink from %LOCALAPPDATA%\SaferVPN\Log is followed. | 2020-09-18 | 5.5 | CVE-2020-25744 MISC MISC |
| uniqlo -- uniqlo | UNIQLO App for Android versions 7.3.3 and earlier allows remote attackers to lead a user to access an arbitrary website via a malicious App created by the third party. As a result, if the access destination is a malicious website, the user may fall victim to the social engineering attack. | 2020-09-18 | 4.3 | CVE-2020-5629 MISC |
| uniqlo -- uniqlo | UNIQLO App for Android versions 7.3.3 and earlier allows remote attackers to lead a user to access an arbitrary website via the vulnerable App. As a result, if the access destination is a malicious website, the user may fall victim to the social engineering attack. | 2020-09-18 | 4.3 | CVE-2020-5628 MISC |
| webtareas_project -- webtareas | webTareas through 2.1 allows XSS in clients/editclient.php, extensions/addextension.php, administration/add_announcement.php, administration/departments.php, administration/locations.php, expenses/claim_type.php, projects/editproject.php, and general/newnotifications.php. | 2020-09-18 | 4.3 | CVE-2020-25735 MISC MISC MISC |
| webtareas_project -- webtareas | webTareas through 2.1 allows upload of the dangerous .exe and .shtml file types. | 2020-09-18 | 5 | CVE-2020-25733 MISC MISC MISC |
| webtareas_project -- webtareas | webTareas through 2.1 allows files/Default/ Directory Listing. | 2020-09-18 | 5 | CVE-2020-25734 MISC MISC MISC |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In netd, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137346580 | 2020-09-18 | 2.1 | CVE-2020-0365 MISC |
| google -- android | In Telecom, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155650969 | 2020-09-18 | 2.1 | CVE-2020-0295 MISC |
| google -- android | In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction are needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-144506224 | 2020-09-18 | 3.5 | CVE-2020-0282 MISC |
| google -- android | In the Accessibility service, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154913130 | 2020-09-18 | 2.1 | CVE-2020-0263 MISC |
| google -- android | In Telephony, there are possible leaks of sensitive data due to missing permission checks. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-150155839 | 2020-09-18 | 2.1 | CVE-2020-0265 MISC |
| google -- android | In Android Auto Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645626 | 2020-09-18 | 2.1 | CVE-2020-0269 MISC |
| google -- android | In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253784 | 2020-09-18 | 2.1 | CVE-2020-0284 MISC |
| google -- android | In Telephony, there is a possible permission bypass due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-156253479 | 2020-09-18 | 2.1 | CVE-2020-0285 MISC |
| google -- android | In the wallpaper manager, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154915372 | 2020-09-18 | 2.1 | CVE-2020-0294 MISC |
| google -- android | In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151646375 | 2020-09-18 | 2.1 | CVE-2020-0302 MISC |
| google -- android | In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure. System execution privileges, a Firmware compromise, and User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137857778 | 2020-09-18 | 3.5 | CVE-2020-0281 MISC |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645695 | 2020-09-18 | 2.1 | CVE-2020-0304 MISC |
| google -- android | In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-151645867 | 2020-09-18 | 2.1 | CVE-2020-0307 MISC |
| google -- android | In Settings, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153356468 | 2020-09-18 | 2.1 | CVE-2020-0310 MISC |
| google -- android | In InputManagerService, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-153878642 | 2020-09-18 | 2.1 | CVE-2020-0311 MISC |
| google -- android | In NotificationManagerService, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154917989 | 2020-09-18 | 2.1 | CVE-2020-0313 MISC |
| google -- android | In Zen Mode, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-155642026 | 2020-09-18 | 2.1 | CVE-2020-0315 MISC |
| google -- android | In Telephony, there is a missing permission check. This could lead to local information disclosure of radio data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-154934919 | 2020-09-18 | 2.1 | CVE-2020-0316 MISC |
| google -- android | In NFC, there is a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-145079309 | 2020-09-18 | 2.1 | CVE-2020-0325 MISC |
| google -- android | In Settings, there is a possible permissions bypass. This could lead to local information disclosure of the device's IMEI with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-147309310 | 2020-09-18 | 2.1 | CVE-2020-0331 MISC |
| google -- android | In NFC, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-139188779 | 2020-09-18 | 2.1 | CVE-2020-0349 MISC |
| ibm -- data_risk_manager | IBM Data Risk Manager (iDNA) 2.0.6 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: 184928. | 2020-09-22 | 3.5 | CVE-2020-4615 XF CONFIRM |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ozeki -- ozeki_ng_sms_gateway | An issue was discovered in Ozeki NG SMS Gateway through 4.17.6. The database connection strings accept custom unsafe arguments, such as ENABLE_LOCAL_INFILE, that can be leveraged by attackers to enable MySQL Load Data Local (rogue MySQL server) attacks. | 2020-09-22 | 3.5 | CVE-2020-14027 MISC MISC |
| philips -- clinical_collaboration_platform | Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output used as a webpage that is served to other users. | 2020-09-18 | 2.7 | CVE-2020-14525 MISC |
| philips -- clinical_collaboration_platform | Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an attacker to influence the amount of resources consumed, eventually leading to the exhaustion of available resources. | 2020-09-18 | 3.3 | CVE-2020-16200 MISC |
| philips -- clinical_collaboration_platform | Philips Clinical Collaboration Platform, Versions 12.2.1 and prior. The product exposes a resource to the wrong control sphere, providing unintended actors with inappropriate access to the resource. | 2020-09-18 | 3.6 | CVE-2020-16247 MISC |