CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: WirelessHART-Gateway– Vulnerability may allow remote attackers to cause a Denial Of Service

Document ID TDOCT-7268_ENG
Publication date 2021-08-16

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2021-33555	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	The filename parameter is vulnerable to unauthenticated path traversal attacks, enabling read access to arbitrary files on the server.
CVE-2020-11023	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.
CVE-2020-11022	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-7656	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.
CVE-2019-11358	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
CVE-2016-10707	CWE-400: Uncontrolled Resource Consumption	jQuery 3.0.0-rc.1 is vulnerable to Denial of Service (DoS) due to removing a logic that lowercased attribute names. Any attribute getter using a mixed-cased name for boolean attributes goes into an infinite recursion, exceeding the stack call limit.

Identifier	Vulnerability Type	Description
CVE-2015-9251	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
CVE-2014-6071	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jQuery 1.4.2 allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to use of the text method inside after.
CVE-2012-6708	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion.
CVE-2011-4969	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.
CVE-2007-2379	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	The jQuery framework exchanges data using JavaScript Object Notation (JSON) without an associated protection scheme, which allows remote attackers to obtain the data via a web page that retrieves the data through a URL in the SRC attribute of a SCRIPT element and captures the data using other JavaScript code, aka "JavaScript Hijacking."
CVE-2021-34559	CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	Rewriting of links and URLs in cached pages to arbitrary strings by unauthenticated HTTP clients
CVE-2021-34560	CWE-200: Information Exposure	The form contains the following password field with autocomplete enabled: password. The stored credentials can be captured by an attacker who gains control over the user's computer. Therefore the user must have logged in at least once.
CVE-2021-34561	CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action	This is a serious issue if the application is not externally accessible or uses IP-based access restrictions. Attackers can use DNS Rebinding to bypass any IP or firewall based access restrictions that may be in place, by proxying through their target's browser.
CVE-2021-34562	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	It is possible to inject arbitrary JavaScript into the application's response

Identifier	Vulnerability Type	Description
CVE-2021-34563	CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag	The HttpOnly attribute is not set on a cookie, then the cookie's value can be read or set by client-side JavaScript.
CVE-2021-34564	CWE-315: Cleartext Storage of Sensitive Information in a Cookie	Any cookie-stealing vulnerabilities within the application or browser would enable an attacker to steal the user's credentials to the application.
CVE-2013-0169	CWE-310: Cryptographic Issues	The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.
CVE-2021-34565	CWE-798: Use of Hard-coded Credentials	SSH and Telnet service is active with hard-coded credentials.

Severity

Identifier	Base Score and Vector
CVE-2021-33555	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2020-11023	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2020-11022	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2020-7656	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2019-11358	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2016-10707	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVE-2015-9251	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2014-6071	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2012-6708	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2011-4969	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2007-2379	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CVE-2021-34559	5.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)
CVE-2021-34560	5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)
CVE-2021-34561	7.5 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)
CVE-2021-34562	5.4 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)
CVE-2021-34563	3.3 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N)
CVE-2021-34564	5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)
CVE-2013-0169	2.6 (CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVE-2021-34565	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Affected products

Item No.	Item	Firmware Version	Affected by
217229	WHA-GW-F2D2-0-AS-Z2-ETH	3.0.7	CVE-2020-11023, CVE-2020-11022, CVE-2020-7656, CVE-2019-11358, CVE-2016-10707, CVE-2015-9251, CVE-2014-6071, CVE-2012-6708, CVE-2011-4969, CVE-2007-2379, CVE-2021-33555, CVE-2021-34559, CVE-2021-34560, CVE-2021-34561, CVE-2021-34565
252863	WHA-GW-F2D2-0-AS-Z2-ETH.EIP	3.0.8	CVE-2020-11023, CVE-2020-11022, CVE-2020-7656, CVE-2019-11358, CVE-2016-10707, CVE-2015-9251, CVE-2014-6071, CVE-2012-6708, CVE-2011-4969, CVE-2007-2379, CVE-2021-34559, CVE-2021-34560, CVE-2021-34561, CVE-2021-34562, CVE-2021-34563, CVE-2021-34565
		3.0.9	CVE-2021-34560, CVE-2021-34563, CVE-2021-34564, CVE-2013-0169, CVE-2021-34565

Summary

Critical vulnerabilities have been discovered in the product and in the utilized components jQuery by jQuery Team and TLS Version 1.0/1.1.

The impact of the vulnerabilities on the affected device may result in
- denial of service
- remote code execution
- code exposure

Impact

Pepperl+Fuchs analyzed and identified affected devices.
Remote attackers may exploit the vulnerability sending specially crafted packages that may result in a denial-of-service condition or code execution.

Solution

An external protective measure is required.

- Minimize network exposure for affected products and ensure that they are not accessible via the Internet.
- Isolate affected products from the corporate network.
- If remote access is required, use secure methods such as virtual private networks (VPNs).

Reported by

Pepperl+Fuchs
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.