

# Regarding several security vulnerabilities in our HEMS

January 30, 2024

SHARP CORPORATION

Thank you for using Sharp's Energy Management Controller with Cloud Services.

Recently, several security vulnerabilities have discovered in Sharp's Energy Management Controller with Cloud Services. Please see the table below for an overview of the vulnerabilities and the possible effects.

We sincerely apologize for any inconvenience to our customers.

<b>Vulnerability identification number</b>	JVNVU#94591337
<b>Applicable product name and version</b>	Product name: Energy Management Controller with Cloud Services Model name: JH-RVB1 /JH-RV11 Version: Ver.B0.1.9.1 or before
<b>Conditions for attack</b>	In order for an attack that exploits these vulnerabilities to be successful, a computer that is the origin of the attack must be connected to the same network as the product installed. In cases other than the above, there could be no impact from these vulnerabilities.
<b>Possible effects</b>	There is a risk that a malicious attacker could leak the product's configuration information and/or customer's home power information, or make unintentional changes to the product's configuration information, or the product could be an origin for any other cyberattacks.
<b>Impact mitigation measures</b>	If you are using this product, please do not connect the product directly to the Internet, but use it within a network protected by a router, etc. If you are using a wireless LAN router, please take measures such as configuring newer encryption methods (WPA2 Personal (AES) or later is recommended), changing the administrative password from the default, and keeping the firmware up to date. We do not recommend using wireless LAN routers that only support older encryption methods. If you have personal computers that connected to the same network, please update the OS regularly, install a security software, and keep its definition files up to date. By taking these measures, you can mitigate the risk of being affected above possibility.

<b>How to respond</b>	<p>In environments where the Energy Management Controller with Cloud Services is connected to the Internet, the latest version will be updated automatically.</p> <p>The firmware version after fixing these vulnerabilities is Ver.B0.2.0.0 or later.</p> <p>Inquiries regarding this matter <a href="https://jp.sharp/support/taiyo/">https://jp.sharp/support/taiyo/</a></p>
<b>Acknowledgment</b>	<p>These vulnerabilities were discovered by Shoji Baba of GMO Cybersecurity by Ierae, Inc. reported via JPCERT/CC. Thank you very much for that report.</p>
<b>Information</b>	<b>JVNVU#94591337</b>