

## 有关本公司可编程显示器多个脆弱性的事宜

IDEC 株式会社

公布日期 2024 年 8 月 29 日

## ■ 概述

本公司的可编程显示器中存在因 TCP/IP 堆栈引起的多个漏洞。

## ■ 该产品的确认方法

该产品及软件版本如下。

产品	软件版本
HG5G/4G/3G/2G-V 型 可编程显示器	Ver. 4.85 及更早
HG4G/3G 型可编程显示器	Ver. 4.85 及更早
HG2G-5F 型可编程显示器	Ver. 4.85 及更早
HG2G-5T 型可编程显示器	Ver. 4.85 及更早
HG1G 型可编程显示器	Ver. 4.85 及更早
HG1P 型可编程显示器	Ver. 4.85 及更早

## ■ 脆弱性的说明

本公司的可编程显示器使用的是图研 ELMIC 公司生产的 TCP/IP 堆栈，而 TCP/IP 堆栈存在以下已知漏洞（通常称为“URGENT/11”及“Ripple20”）。

CVE-2019-12264	CVE-2020-11908
CVE-2020-11901	CVE-2020-11909
CVE-2020-11903	CVE-2020-11910
CVE-2020-11904	CVE-2020-11911
CVE-2020-11906	CVE-2020-11912
CVE-2020-11907	CVE-2020-11914

## ■ 脆弱性带来的威胁

第三方可能会被执行任意代码、信息窃取或者受到服务运行干扰攻击（Dos）。

**■对策方法**

已修复漏洞的产品及软件版本如下。

产品	软件版本
HG5G/4G/3G/2G-V 型 可编程显示器	Ver. 4.86 及更高
HG4G/3G 型可编程显示器	Ver. 4.86 及更高
HG2G-5F 型可编程显示器	Ver. 4.86 及更高
HG2G-5T 型可编程显示器	Ver. 4.86 及更高
HG1G 型可编程显示器	Ver. 4.86 及更高
HG1P 型可编程显示器	Ver. 4.86 及更高

请从本公司的主页下载各软件的最新版本进行更新。

**■缓解措施・回避措施**

为了最大限度的降低利用此漏洞的风险，请使用专用网络或 VPN 等封闭网络。详情请参阅本公司主页上的“[安全注意事项](#)”。

**■更新履历**

2024 年 8 月 29 日 公布了此脆弱性信息页面。

**■咨询方式**

请通过本公司主页进行咨询。