Information History

No	Detail
1	The login function on this website was deleted on April 23rd, 2018. User's information which was registered when they registered their accounts was deleted in May, 2018.
2	Epson Security Notification **[Privilege Escalation Vulnerability]** CVE-2015-6034 (Release Date: 10/21/15) http://www.kb.cert.org/vuls/id/672500 **[Description]** The EPSON Network utility included with some older Epson printers installs a binary with weak permissions, which can allow a low privilege user to escalate their privileges and take control of the system. **[Impact]** Successful exploitation of this vulnerability can lead to unauthorized control of the system by a low privilege user. **[Affected Products for ColorWorks category in this website]** - GP-C830, GP-C831, GP-C832, GP-M800, GP-M830, GP-M831, GP-M832 - TM-C3400, TM-C3500, TM-C3510, TM-C3520 - TM-C7500, TM-C7510, TM-C7520, TM-C7500G, TM-C7510G, TM-C7520G **[Affected Contents]** - Printer Driver for TM-C3400 - Printer Driver for TM-C3500/C3510/C3520 - TM-C35x0 Compressed data Driver - TM-C3500 Series Install Navi - Epson Inkjet Label Printer SDK (TM-C3400, TM-C3400BK, TM-C3500 Series, TM-C7500 Series, TM-C7500G Series) - EPSON Monitoring Tool **[Solution]** To ensure the security of your Epson software, please download and install the patch program for privilege escalation vulnerability of EPSON Network Utility. https://download.epson-biz.com/?content=securitypatch_enu_pos
3	**[Authentication Bypass Vulnerability]** Reference CVE-2022-36133 : This will be published soon. **[Description]** An exploitable authentication bypass vulnerability exists in the WebConfig functionality of some Epson printers. **[Impact]** A successful attack would allow the attacker to change the printer's communication settings. A printer whose communication settings have been changed becomes temporarily unusable. **[Affected Printers]** - TM-C3500 - TM-C7500 **[Solution]** To ensure the security of your printer, please download and apply the latest firmware updater. - TM-C3500 - TM-C7500 **[Acknowledgments]** We would like to thank Evgeni Sabev from SAP Global Security for responsibly disclosing these vulnerabilities to us.