ZEBRA

Zebra Technologies Corporation
3 Overlook Point
Lincolnshire, IL 60069

p 847-634-6700
f 847-913-8766
zebra.com

9-27-2017

Dear Valued Zebra Customers,

Topic or Information: BlueBorne, Wormable Bluetooth Attack

Applies To: All Zebra Printer Products

Conclusion: Zebra's Product Security team has verified that all printer products, Link-OS™ printers and CAG specials released after January 1st, 2013 are not susceptible to this form of attack. We are continuing to investigate the susceptibility of our earlier printer platforms and will revise this notification as more information is made available.

Overview: Zebra Technologies Corporation ("Zebra") is aware of a new Bluetooth vulnerability that could potentially expose millions of devices to remote attack. A security firm Armis has identified a set of 8 zero-day vulnerabilities which put Bluetooth-capable devices at the risk of being compromised. Armis considers four of these vulnerabilities as critical since they can allow attackers to take control of users' devices, steal confidential data, access corporate networks, perform remote code execution and MITM attacks, spread malware to nearby devices, and even penetrate "air-gapped" networks.

Dubbed "BlueBorne", the attack works by masquerading as a Bluetooth device and exploiting specific protocol weaknesses to deploy malicious code into the product. Even air-gapped devices or networks that aren't connected to the internet are vulnerable, since Bluetooth is a wireless proximity communications method that doesn't require the device to be in discoverable mode or paired with the attacker's device to be vulnerable. Zebra recommends carefully considering the services and communication ports that are active on your devices. If a given port or service is not necessary for your application, consider turning it off.

Sincerely,

DocuSigned by:
James M Rehberger
76E3EBD4F61C46E...

James M. Rehberger

Director, AIT Product and Information Security