B

BlueBorne: Bluetooth Vulnerabilities and Protection

What it is BlueBorne is the name given to a group of Bluetooth implementation vulnerabilities disclosed in 2017. It is not one virus or malware family. The flaws affected several platforms, including versions of Android, Linux, Windows...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

BlueBorne is the name given to a group of Bluetooth implementation vulnerabilities disclosed in 2017. It is not one virus or malware family. The flaws affected several platforms, including versions of Android, Linux, Windows, and iOS, and could allow attacks over Bluetooth without the normal pairing process in some conditions.

How it works

A nearby attacker can probe the Bluetooth stack and, depending on the device and unpatched flaw, may trigger information disclosure, code execution, or a man-in-the-middle condition. Range, platform, and exploit requirements differ by vulnerability. A device being non-

discoverable did not necessarily remove exposure in the originally affected implementations.

Key points

- The practical risk depends on the exact operating-system version and whether the vendor patch is installed.
- Bluetooth names and pairing prompts are not reliable proof that a nearby device is safe.
- Modern patched devices are not automatically vulnerable merely because Bluetooth is enabled.

What to do

- Install current operating-system and firmware updates from the device vendor.
- Disable Bluetooth when it is not needed, especially on unsupported legacy devices.
- Remove unknown pairings and investigate unexpected Bluetooth behavior or repeated connection prompts.
- Segment unmanaged and IoT devices so one compromised device cannot freely reach sensitive systems.

What protection still matters

BlueBorne refers to a group of disclosed Bluetooth implementation vulnerabilities, not one downloadable malware family. Exposure depends on the device, operating-system build, Bluetooth stack, and vendor patch status. Install current OS and firmware updates, retire unsupported devices, and disable Bluetooth when it is not needed in high-risk locations. Do not rely only on hidden or non-discoverable mode because some flaws can be reached without normal pairing. Inventory embedded and IoT devices as well as phones and laptops. A verified vendor software patch is the primary fix; scanning cannot repair a vulnerable Bluetooth stack.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com