B

BlueBorne Bluetooth Vulnerabilities: Affected Devices, Checks, and Mitigation

BlueBorne is a set of Bluetooth vulnerabilities disclosed in 2017, not one virus. Learn which devices may remain at risk, how to verify patch status, and how to mitigate unsupported products.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
5 min

CONTENTS

In this guide

BlueBorne is the name given to a group of Bluetooth implementation vulnerabilities disclosed by Armis in 2017. It is not one virus and not one CVE. The original research covered flaws affecting implementations in Android, Linux, Windows, and Apple platforms, with impact ranging from information disclosure and man-in-the-middle conditions to code execution.

The practical risk today depends on the exact device, operating-system build, Bluetooth stack, vendor patch, and whether the product is still supported. Current supported phones and computers generally received fixes long ago. Older phones, embedded devices, medical equipment, vehicles, televisions, and other IoT products may be difficult or impossible to patch.

01 How the BlueBorne attack vector works

1. An attacker is within Bluetooth radio reach of a vulnerable device.
2. The attacker discovers or interacts with the device's Bluetooth implementation.
3. A matching vulnerability is exploited; documented cases did not always require pairing or a user opening a file.

4. Depending on the platform and flaw, the attacker may obtain information, intercept traffic, crash a service, or execute code.
5. A compromised device could be used for further activity on networks and systems it can reach.

Bluetooth radio range varies with hardware, obstacles, interference, and equipment. Do not rely on a single fixed distance as a security boundary.

02 BlueBorne is a vulnerability set, not a malware family

Statement	Accurate interpretation
"BlueBorne virus"	Informal wording; BlueBorne refers to vulnerabilities and an attack vector, not a self-contained virus
"One BlueBorne patch"	Vendors released platform-specific updates for different flaws and products
"Bluetooth must be paired"	Some documented vulnerabilities could be reached without an existing paired relationship
"Bluetooth icon is hidden"	Discoverability and visibility are not the same as disabling the Bluetooth radio or patching the stack
"A scanner says safe"	Inventory tools can help, but vendor build and patch evidence determine support status

03 Which devices may be affected?

The original disclosure described issues across major Bluetooth stacks used by Android, Linux, Windows, iOS, and related products. Whether a particular device remains vulnerable cannot be decided from the brand name alone.

- Record the exact manufacturer, model, hardware revision, operating-system or firmware version, and security patch level.

- Check the device vendor's security advisory and update history for that exact product.
- Confirm whether the product is still supported and whether an update can actually be installed.
- For managed systems, use inventory and vulnerability-management data rather than asking users to self-report only the device name.
- Treat unsupported Bluetooth-enabled devices as a lifecycle risk even if no active exploit is observed.

Some devices use vendor-customized Bluetooth components or embedded chipsets, so the operating-system version alone may not tell the complete story.

04 How to check and reduce BlueBorne risk

1. **Install all vendor updates.** Update the operating system, firmware, Bluetooth drivers, and device-management components from official sources.
2. **Verify the patch level.** A device reporting "up to date" may only mean it has the newest release that its now-unsupported model is allowed to receive.
3. **Disable Bluetooth when it is not required.** Use the actual system control or management policy; hiding discoverability alone is not equivalent.
4. **Remove unnecessary pairings.** This does not patch BlueBorne, but it reduces other Bluetooth trust and impersonation risks.
5. **Segment embedded and IoT devices.** Limit what an exploited product could reach on internal networks.
6. **Monitor unusual behavior.** Watch for unexpected Bluetooth service crashes, new network activity, changed configurations, and endpoint detections.
7. **Replace unsupported products.** If Bluetooth cannot be disabled and no vendor fix exists, replacement may be the only durable mitigation.

05 Does turning Bluetooth off fix BlueBorne?

Turning Bluetooth off removes the wireless attack path while the radio remains disabled, but it does not install a security patch. The risk returns if Bluetooth is enabled again. Some devices or accessories may reactivate Bluetooth for features, setup, or updates, so managed policy and verification are preferable.

Airplane mode behavior varies by platform and user settings. Confirm that Bluetooth is actually off rather than assuming the airplane icon guarantees it.

06 What to do if exploitation is suspected

1. **Disable Bluetooth and isolate the device from networks.**
2. **Record the device details.** Preserve model, OS/firmware build, patch level, time, location, alerts, crashes, and nearby-device observations.
3. **Review external telemetry.** Check network, identity, mobile-device-management, endpoint, and application logs because the device may not reliably show all activity.
4. **Protect accounts and keys.** Revoke exposed sessions, rotate credentials used on the device, and replace certificates or tokens when evidence warrants it.
5. **Apply vendor recovery guidance.** Update, reset, reimage, or replace the device depending on platform support and the assessed compromise.
6. **Investigate reachable systems.** Look for lateral movement or unusual access originating from the device after the suspected event.

There is no universal "BlueBorne removal tool." The vulnerabilities are repaired through vendor updates; any payload or follow-on compromise must be handled with platform-appropriate incident response.

07 Enterprise BlueBorne checklist

- Inventory Bluetooth-capable laptops, phones, scanners, printers, access points, sensors, and specialized equipment.

- Track product support dates and require minimum OS and patch levels.
- Disable unused Bluetooth through configuration management.
- Place unpatchable operational and IoT devices in restricted network segments.
- Document business owners and replacement plans for unsupported equipment.
- Test monitoring and incident-response coverage for devices that cannot run endpoint agents.
- Include Bluetooth exposure in procurement and vendor-security requirements.

08 Frequently asked questions

Is BlueBorne still relevant?

It remains relevant mainly for old, unsupported, embedded, or poorly managed devices. Supported products should be updated, but organizations must verify rather than assume every Bluetooth device received a fix.

Can BlueBorne attack a device that is not discoverable?

The original research showed that hiding normal discoverability was not a sufficient defense for affected implementations. Disable Bluetooth or install the vendor patch.

Does antivirus block BlueBorne?

Endpoint protection may detect payloads or follow-on behavior, but the primary fix is the vendor's operating-system, driver, or firmware update.

Is BlueBorne the same as BLEEDINGBIT?

No. Both concern Bluetooth-related security, but BLEEDINGBIT is a separate set of vulnerabilities disclosed later for certain Bluetooth Low Energy chips and products.

09 References

- Armis: BlueBorne one year later
- Android Security Bulletin: September 2017

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