contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Microsoft Windows exploited

CVE-2026-96951 · on CISA's exploited list since 13 October 2026

Analysis Report

If you run Windows 10 Version 1607 or 1809, Microsoft Edge or Outlook.com, act now: CISA's deadline was 16 October 2026. First, find which builds you run and ask your IT provider whether the vendor's …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.8**	STATUS	On CISA's exploited list; due 16 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/microsoft-windows-cve-2026-96951

The bottom line

> *If you run Windows 10 Version 1607 or 1809, Microsoft Edge or Outlook.com, act now: CISA's deadline was 16 October 2026. First, find which builds you run and ask your IT provider whether the vendor's fix is installed.*

At a glance

Fact	Detail
Product	Microsoft Windows (CVE-2026-96951)
Severity	High: 8.8 (CVSS 3.1)
CISA	On its exploited list since 13 October 2026. Deadline for US federal agencies: 16 October 2026.
Chance of exploitation (EPSS)	0.10, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The record's affected ranges end before 154.0.4258.62, 20260925.100, 10.0.14393.9612, 10.0.17763.9376
Who looks first	Anyone running Windows 10 Version 1607 or 1809, Microsoft Edge (Chromium-based) or Outlook.com, as the record lists them. The record names no further condition.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Windows 10 Version 1607 or 1809 on any machine?	Go to the next question about Edge.	Check the build number (next question).
Is any of those machines below build 10.0.14393.9612 (1607) or 10.0.17763.9376 (1809)?	Those releases are outside the record's ranges. Nothing more for them.	Treat it as affected and ask your provider to update it now.
Do you run Microsoft Edge (Chromium-based) below 154.0.4258.62?	Nothing to do for Edge on this CVE.	Treat it as affected and ask your provider to update it.

Does anyone in your firm use Outlook.com for work mail?	Nothing to do for Outlook.com.	Ask your provider or Microsoft support what status the service shows.

What it is

The record says a flaw in Windows Shell lets an unauthorised attacker, over a network, bypass a security feature by passing special characters into a command without proper checking. It does not say which feature is bypassed.

Why it matters

Our reading is that a way past a security feature, reachable over a network, lets an attacker skip a check that was meant to stop them. The record does not say which feature, or how an attack runs. The affected list covers a browser, a mail service and two named Windows 10 releases, so exposure may be wide. With no vendor advice read, applying the vendor's update is the only sure answer.

Things people will get wrong

- "It only bypasses a security feature, so it is minor." The record scores it 8.8 on CVSS 3.1, and CISA lists it as exploited. The record does not say which feature is bypassed, so you cannot judge the damage.
- "Our Windows is not in the list, so we are safe." The record names only two Windows 10 releases, but it also names Edge and Outlook.com. Check all of them before you stop.
- "A command injection needs someone to log in first." The description says an unauthorised attacker, over a network. The record names no login requirement.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- List every Windows 10 machine and note whether it is Version 1607 or 1809, and its build number.
- Find the Edge version on staff machines, because the record gives a fixed build boundary for it.

Step 2: Reduce exposure while you wait

- Ask your provider which of these machines can be reached from the internet or by untrusted people, and handle those first.
- CISA says to apply the vendor's mitigations. The vendor's own instructions were not available to us, so ask your provider for them.

Step 3: Apply the vendor's update

- Ask your provider to install the vendor's security update on each affected machine, then restart where needed.
- No source we read names the fixed version, so ask for it in writing.

Step 4: Check and record

- Re-run the version checks and compare against the record's ranges.
- Keep the results with the date, in case you need to show what was done.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, CISA lists CVE-2026-96951, a command injection flaw in Windows Shell, as exploited, with a deadline of 16 October 2026. Please tell us whether we run Windows 10 Version 1607 or 1809, Microsoft Edge or Outlook.com, and on which machines. Please give the version or build on each. Please also name the fixed version from Microsoft's advisory and confirm in writing that it is installed, by a date you propose. If any machine cannot be updated, please tell us why and what you have done instead. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected commands started by Windows Shell on affected machines, since the description points to a command being built from unchecked input.

- Network connections to affected machines from unfamiliar sources before they were updated.

The weakness behind it

The record classes this as CWE-77 (Improper Neutralization of Special Elements used in a Command).

The sources, in their words

CISA's catalogue entry:

> *Microsoft Windows Shell contains a command injection vulnerability that allows an unauthorized attacker to bypass a security feature over a network.*

The CVE record, published by Microsoft on 13 October 2026:

> *Improper neutralization of special elements used in a command ('command injection') in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.*

Versions of Microsoft Edge (Chromium-based) the record lists as affected:

- 1.0.0.0 up to, but not including, 154.0.4258.62

The affected ranges end before 154.0.4258.62. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Microsoft Outlook.com the record lists as affected:

- 1.0.0 up to, but not including, 20260925.100

The affected ranges end before 20260925.100. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Microsoft Windows 10 Version 1607 the record lists as affected:

- 10.0.14393.0 up to, but not including, 10.0.14393.9612

The affected ranges end before 10.0.14393.9612. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Microsoft Windows 10 Version 1809 the record lists as affected:

- 10.0.17763.0 up to, but not including, 10.0.17763.9376

The affected ranges end before 10.0.17763.9376. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which security feature is bypassed, and what an attacker gains once it is bypassed.
- The fixed version for each product. No vendor page was read, and the record lists no unaffected versions.
- How the attack is carried out, and whether it needs a user to click or open anything.
- Whether any workaround exists short of updating.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-96951: score 8.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	Required	A person must click, visit or open something.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
13 October 2026	CVE record published by Microsoft.
13 October 2026	CISA added it to its list of exploited vulnerabilities.
16 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
A Windows 10 Version 1607 or 1809 machine below the build numbers in the record	High	Now; CISA's deadline has passed
Edge (Chromium-based) below 154.0.4258.62 on staff laptops	High	Now; CISA's deadline has passed
Staff who use Outlook.com for work mail	Medium	This week; ask for the service status

Other Windows releases not named in the record	Low	Next patch cycle; confirm with your provider
No Windows 10 1607 or 1809, no Edge, no Outlook.com	None	None for this CVE

Appendix 4. Definition of done

- Every Microsoft Windows you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-96951: https://www.cve.org/CVERecord?id=CVE-2026-96951
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951