cyberscore

CONTINUOUS VALIDATION · SAMPLE

When you are affected

The two messages a customer receives when a major vulnerability is published in a product they run. First an automatic heads-up, then the verdict from a specialist.

This is a sample. Example Company B.V., the product ExampleGate VPN and the vulnerability EXAMPLE-2026-0001 do not exist. The layout and wording are those of the real messages, which are sent as plain text.

01 The heads-up, sent automatically

Sent the moment our matching finds the product in the customer's inventory. It names the systems and the time by which the verdict follows. It is not a verdict and says so.

From CyberScore verdicts <verdicts@cyberscore.nl>
To it@example-company.example, ciso@example-company.example
Sent Monday 23 November 2026, 10:37
Subject [Heads-up] EXAMPLE-2026-0001 · ExampleGate VPN · your verdict follows by Mon 23 Nov, 17:00

```
A major vulnerability was published in a product that is in your inventory.

Product:               ExampleGate VPN
Vulnerability:         EXAMPLE-2026-0001 · Sign-in bypass in the web portal
Exploited in attacks:  Yes
Your systems with it:  vpn-ams-01, vpn-fra-01, vpn-lab-01
Inventory as of:       18 November 2026

What happens now
A certified security specialist is checking these systems against the
vulnerability. You receive your verdict by Monday 23 November 2026, 17:00 CET.

This message is not a verdict. It was sent automatically, the moment our
matching found the product in your inventory. Your systems may turn out not
to be affected.

Background: https://exampleco.example/advisories/2026-01

Questions: reply to this message.
```

02 The verdict, written and approved by a specialist

One line per system: the version we found, whether it can be reached from the internet, the verdict, what to do and by when. In this sample the customer has the Validate package, so proof by testing follows.

From CyberScore verdicts <verdicts@cyberscore.nl>
To it@example-company.example, ciso@example-company.example
Sent Monday 23 November 2026, 15:10
Subject [Affected] EXAMPLE-2026-0001 · ExampleGate VPN · first action today

```
Your verdict: Affected
Based on your inventory as of 18 November 2026. 2 of your 3 ExampleGate VPN systems run a vulnerable version.

System     | Version found | Reachable from the internet | Verdict      | Action                                                  | By when
-----------+---------------+-----------------------------+--------------+---------------------------------------------------------+-------------------------------------
vpn-ams-01 | 9.2.1         | Yes                         | Affected     | Switch off the web portal today, then patch to 9.2.5 | Portal off today, patch by Thu 26 Nov
vpn-fra-01 | 9.2.4         | Yes                         | Affected     | Switch off the web portal today, then patch to 9.2.5 | Portal off today, patch by Thu 26 Nov
vpn-lab-01 | 9.2.5         | No                          | Not affected | None                                                    |

Proof by testing follows within 2 working days.

Checked by a certified security specialist on 23 November 2026.

Background: https://exampleco.example/advisories/2026-01

Questions: reply to this message.
```

What else happens

- **We also call.** When a customer is affected by a vulnerability that is being exploited, as in this sample, we call as well as write.
- **Proof follows.** In Validate and Embedded we test within 2 working days whether the weakness can really be used, and send what we found.
- **The score moves the same day.** The finding counts towards the Cyberscore from the day of the verdict.
- **We retest the fix.** The finding closes only when our retest passes.

The other two verdicts are *Not affected* (no action needed, with the systems we checked) and *Checking* (we need one answer from you, and say which).

Questions: info@cyberscore.nl · +31 229 842 113