

# Daily Threat Bulletin

15 October 2026

## Vulnerabilities

### [Palo Alto Networks warns of PAN-OS RCE flaw exploited in attacks](#)

BleepingComputer - 14 October 2026 19:56

Palo Alto Networks has released security updates for a high-severity PAN-OS RCE zero-day, tracked as CVE-2026-0322, that has been exploited in attacks targeting firewalls.

### [Cisco patches new Secure Email Gateway zero-day exploited in attacks](#)

BleepingComputer - 14 October 2026 14:29

Cisco has patched another actively exploited zero-day flaw in its Secure Email Gateway (SEG) that lets remote unauthenticated attackers execute commands with root privileges.

### [CISA Urges Immediate Ivanti Connect Secure Updates as Honeypots Log 105 Exploit Attempts](#)

The Hacker News - 14 October 2026 19:00

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday urged organizations to take steps to immediately update their Ivanti Connect Secure (ICS) appliances and deployments to the latest version following the disclosure of an actively exploited vulnerability.

### [Hackers Backdoor Nextcloud Servers Through Critical Flaw in Collabora's Built-in CODE App](#)

The Hacker News - 15 October 2026 00:08

Attackers exploited a flaw in an optional Nextcloud app, Collabora Online - Built-in CODE Server, to plant web shells on Nextcloud servers. Three administrators reported the issue on GitHub, with the first logged attack on September 10.

### [Microsoft Breaks Patch Tuesday Record Again with 1400+ CVEs](#)

Infosecurity Magazine - 14 October 2026 09:45

Microsoft issued its largest ever round of security updates in the October Patch Tuesday.

### [Chrome, Firefox Updates Patch 114 Flaws as Mozilla Unveils Firefox Enterprise](#)

SecurityWeek - 14 October 2026 08:38

Mozilla has introduced Firefox Enterprise for organizations with strict compliance, governance, and security requirements.



Scottish  
Cyber  
Coordination  
Centre

### **Citrix, Fortinet, Ivanti Patch 29 Vulnerabilities Across Their Products**

SecurityWeek - 14 October 2026 08:26

Critical-severity flaws could lead to authentication bypass, code execution, and sensitive authentication information leaks.

## **Threat actors and malware**

### **Global takedown hits network behind 1 billion phishing messages**

BleepingComputer - 14 October 2026 10:12

A massive cybercriminal ecosystem facilitating more than a billion malicious messages targeting over 75,000 organizations across 150 countries has been disrupted by law enforcement agencies and partners worldwide.

### **Hirudo Android malware replaces banking apps to evade security checks**

BleepingComputer - 14 October 2026 08:41

A new Android malware called Hirudo steals bank account credentials by replacing legitimate banking apps with modified versions that disable security checks.

### **Refrigeration System Cyberattack Impacts 700+ Retailers**

Security Magazine - 14 October 2026 11:20

Security leaders discuss the cyberattack that impacted more than 700 retailers.