



# Daily threat bulletin

1 July 2024

## Vulnerabilities

### [Juniper releases out-of-cycle fix for max severity auth bypass flaw](#)

BleepingComputer - 30 June 2024 12:14

Juniper Networks has released an emergency update to address a maximum severity vulnerability that leads to authentication bypass in Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router products. [...]

### [Hackers exploit critical D-Link DIR-859 router flaw to steal passwords](#)

BleepingComputer - 29 June 2024 12:18

Hackers are exploiting a critical vulnerability that affects all D-Link DIR-859 WiFi routers to collect account information from the device, including passwords. [...]

### [GitLab Releases Patch for Critical CI/CD Pipeline Vulnerability and 13 Others](#)

The Hacker News - 28 June 2024 20:48

GitLab has released security updates to address 14 security flaws, including one critical vulnerability that could be exploited to run continuous integration and continuous deployment (CI/CD) pipelines as any user. The weaknesses, which affect GitLab Community Edition (CE) and Enterprise Edition (EE), have been addressed in versions 17.1.1, 17.0.3, and 16.11.5. The most severe of the

## Threat actors and malware

### [TeamViewer Credits Network Segmentation for Rebuffing APT29 Attack](#)

darkreading - 28 June 2024 22:22

Despite warnings from Health-ISAC and the NCC Group, the remote access software maker says defense-in-depth kept customers' data safe from Midnight Blizzard.

### [Meet Brain Cipher — The new ransomware behind Indonesia's data center attack](#)

BleepingComputer - 29 June 2024 11:14

The new Brain Cipher ransomware operation has begun targeting organizations worldwide, gaining media attention for a recent attack on Indonesia's temporary National Data Center. [...]

### [Unfurling Hemlock Tossing 'Cluster Bombs' of Malware](#)

Security Boulevard - 28 June 2024 22:08



Scottish  
Cyber  
Coordination  
Centre

A threat group dubbed Unfurling Hemlock infects targeted campaign with a single compressed file that, once executed, launches a 'cluster bomb' of as many as 10 pieces of malware that include loaders, stealers, and backdoors. The post Unfurling Hemlock Tossing 'Cluster Bombs' of Malware appeared first on Security Boulevard.

### **Microsoft Alerts More Customers to Email Theft in Expanding Midnight Blizzard Hack**

SecurityWeek - 28 June 2024 17:43

Shockwaves from the Russian government's hack of Microsoft's corporate infrastructure continue to spread as the victim pool widens. The post Microsoft Alerts More Customers to Email Theft in Expanding Midnight Blizzard Hack appeared first on SecurityWeek.