OPEN FORMAL SECURITY ADVISORY

Critical Vulnerabilities Render Certified U.S. Election Systems Insecure

Issued By: Mark Cook
Cybersecurity Professional, 40+ Years Experience
Date: May 13, 2026

I am issuing this formal security advisory to notify all state election officials, the U.S. Election Assistance Commission, federal agencies, and the American public that multiple certified voting systems currently in use across the United States are critically vulnerable to publicly available exploits.

A single independent security researcher operating under the name **Nightmare-Eclipse** has publicly released four powerful exploits: **RedSun**, **BlueHammer**, **UnDefend**, and **YellowKey**. These exploits target multiple critical components of the Windows operating system.

Detailed Breakdown of the Exploits:

- **RedSun** and **BlueHammer**: These are local privilege escalation exploits that allow a standard user to obtain **SYSTEM** level access — the highest level of control on a Windows machine. They abuse flaws in how Windows Defender interacts with files.
- **UnDefend**: Specifically designed to disable or severely degrade **Windows Defender**. It prevents Defender from receiving signature updates and interferes with its core protection mechanisms, effectively weakening or eliminating one of the primary security layers on these systems.
- **YellowKey**: This is not a traditional exploit. It abuses a hidden debug framework that was deliberately left inside Microsoft's Windows Recovery Environment (WinRE). This allows an attacker with physical access to completely bypass BitLocker encryption. The existence of this framework has led many security professionals to question whether it was intentionally designed as a backdoor.

The fact that these severe vulnerabilities were only recently discovered **does not mean they have not been exploited for years**. Zero-day vulnerabilities of this nature can remain undetected for long periods before being publicly disclosed.

Recognition by the Cybersecurity Community

These exploits have already gained significant attention in the professional cybersecurity community. Leading security firms **Huntress** and **Vectra AI** have both published detailed analyses of **BlueHammer**, **RedSun**, and **UnDefend**. Huntress has further confirmed they observed these exact tools being used in real-world enterprise intrusions.

The **YellowKey** BitLocker bypass is much more recent and has not yet received the same level of formal analysis from major firms.

The fact that respected cybersecurity organizations have validated these exploits — and that some have already been used in real attacks — demonstrates that these are not theoretical or exaggerated claims.

Confirmed Vulnerable Certified Systems and Their Exposure:

ES&S (Election Systems & Software)

- **ExpressPoll Electronic Poll Books** (Windows 10 & Windows 11): Vulnerable to all four exploits. ES&S officially lists Windows Defender and BitLocker as core security protections.
- **Electionware EMS and Central Tabulation Systems** (Windows 10 and Windows Server 2016/2019/2022): Vulnerable to RedSun, BlueHammer, and UnDefend.

Dominion Voting Systems

- **Democracy Suite EMS** (versions 5.17, 5.19, 5.20 and state-specific variants) and **ImageCast Central** tabulators (Windows 10, 11, and Windows Server 2019/2022): Vulnerable to RedSun, BlueHammer, and UnDefend. Windows 11 components are also vulnerable to YellowKey. Dominion systems include Windows Defender as part of their standard configuration.

Robis Elections

- **AskED ePollbook** (Windows 10 Pro): Vulnerable to RedSun, BlueHammer, and UnDefend.

VR Systems

- **EViD and EViD Edge Electronic Poll Books** (Windows 10): Vulnerable to RedSun, BlueHammer, and UnDefend.

Clear Ballot Group

- **ClearCount / ClearVote Central Tabulation Workstations** (Windows 10 IoT LTSC): Vulnerable to RedSun, BlueHammer, and UnDefend.

These systems passed federal and state certification testing despite containing these critical, exploitable flaws. This demonstrates that the current testing and certification process is fundamentally inadequate.

A Message to Election Officials:

Election officials are being placed in an impossible and unfair position. You are being held legally and professionally responsible for securing and conducting elections using complex computerized systems that you have neither the technical knowledge, expertise, nor resources to properly evaluate or protect.

You are being set up for failure.

Your sworn duty is to protect the integrity of elections for the citizens you serve. These systems make it nearly impossible for you to fulfill that duty. The only responsible course of action is to demand the immediate removal of these vulnerable systems.

Formal Demand:

I formally demand the **immediate decertification** of all Windows-based voting systems listed in this advisory. The United States must immediately return to transparent, observable elections using in-person voter registration on paper with sole custodianship by county officials digitized in read-only form for public oversight, paper poll books, in-precinct voting on hand-counted paper ballots, and precinct-level vote counting on election night as detailed at **https://handcountroadshow.org/solution**.

This advisory is released publicly and may be freely distributed by any U.S. citizen or election official.

Mark Cook
Cybersecurity Professional (40+ years)

References:

Primary Exploit Sources (Nightmare-Eclipse)

- Nightmare-Eclipse GitHub Repository (main profile): https://github.com/Nightmare-Eclipse
- RedSun Repository: https://github.com/Nightmare-Eclipse/RedSun
- BlueHammer Repository: https://github.com/Nightmare-Eclipse/BlueHammer
- UnDefend Repository: https://github.com/Nightmare-Eclipse/UnDefend
- YellowKey Repository (BitLocker bypass): https://github.com/Nightmare-Eclipse/YellowKey

Major Cybersecurity Company Analyses

- **Huntress** — "Nightmare-Eclipse Tooling Seen in Real-World Intrusion" (April 20, 2026): https://www.huntress.com/blog/nightmare-eclipse-intrusion
- **Vectra AI** — "When the Defender Becomes the Door: BlueHammer, RedSun, and UnDefend in the Wild" (April 20, 2026): https://www.vectra.ai/blog/when-the-defender-becomes-the-door-bluehammer-redsun-and-undefend-in-the-wild

Major Media & Security News Coverage

- Dark Reading — "Exploits Turn Windows Defender Into Attacker Tool": https://www.darkreading.com/cyberattacks-data-breaches/exploits-turn-windows-defender-attacker-tool
- BleepingComputer — "Recently leaked Windows zero-days now exploited in attacks": https://www.bleepingcomputer.com/news/security/recently-leaked-windows-zero-days-now-exploited-in-attacks/
- Help Net Security — "BlueHammer: Windows zero-day exploit leaked": https://www.helpnetsecurity.com/2026/04/08/bluehammer-windows-zero-day-exploit-leaked/

Voting System & Vendor Documentation

- ES&S ExpressPoll Security Fact Sheet: https://www.essvote.com/security_expresspoll/
- Verified Voting Equipment Database: https://verifiedvoting.org/equipmentdb/
- EAC Certified Voting Systems List: https://www.eac.gov/voting-equipment/certified-voting-systems

Additional Technical Coverage

- SOC Prime — "Nightmare-Eclipse PoC Used in Real-World Attacks": https://socprime.com/active-threats/nightmare-eclipse-poc-used-in-real-world-attacks/
- Picus Security — BlueHammer & RedSun analysis
- Cybernews — Coverage of YellowKey release