The Bad: Can You Count the Number of Known Vulnerabilities on Your Enterprise?

Researchers have discovered a new zero-day vulnerability in Ivanti Endpoint Manager (now known as MobileIron Core), allowing remote attackers to obtain Personally Identifiable Information (PII), add admin accounts, and make configuration changes through certain exposed API paths, which can be reached remotely without authentication.

CISA has this week told federal agencies to patch by August 15th. Ubunutu has issued patches for the vulnerabilities as of July 24th and admins are urged to update as soon as possible. Versions susceptible to the bugs range from Ubuntu 18.04 to 23.04. The researchers say that the number of releases available for Ubuntu is over 10,000, and two newly discovered flaws, providing local attackers with ready-made weapons.

Worse, the researchers say that exploits written in 2020 for a similar vulnerability will now work on any Ubuntu instance vulnerable to the bugs. The two flaws, CVE-2023-2640 and CVE-2023-32629, relate to the OverlayFS module in Ubuntu, a popular Linux file system widely used in cloud containers.

The Bad | Millions of Cloud Container Workloads Vulnerable to New Ubuntu Bugs

Companies are not required to reveal specifics about their incident response plans or vulnerabilities such as zero days or n-days that could pose a significant risk to the federal enterprise as malicious cyber actors are known to be exploiting the bug in the wild.

The New Incident Response Rules

The Securities and Exchange Commission has announced that it is adopting new rules that will require publicly-traded companies to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience, and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience, and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience.

The new incident response rules require that publicly-traded companies reveal:

- The impact of the incident on the company's operations
- Any data that may have been compromised, altered, accessed, or used without authorization
- A concise description of the incident's nature and extent
- The date of discovery and status of the incident (ongoing or resolved)
- Information about ongoing or completed remediation efforts by the company
- A description of the company's incident response plans or vulnerabilities such as zero days or n-days that could pose a significant risk to the company
- The number of releases available for Ubuntu

The New Incident Response Rules have been proposed by the SEC with the goal of improving transparency and accountability among public companies. The rules are set to come into force in December.

The Good and the Bad in Cybersecurity: Week 30

The Good:

- The SEC proposes new rules that will require publicly-traded companies to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience.
- The Good: Cybersecurity Predictions 2023 | What's Next?

The Bad:

- The Bad: The Security Incident Response Rules
- The Bad: Ivanti Endpoint Manager patch for mobile devices is vulnerable to a zero-day attack

The Good and the Bad in Cybersecurity: Week 30

The Bad:

- The Bad: Can You Count the Number of Known Vulnerabilities on Your Enterprise?
- The Bad: The Security Incident Response Rules
- The Bad: Ivanti Endpoint Manager patch for mobile devices is vulnerable to a zero-day attack

The Good:

- The Good: The SEC proposes new rules that will require publicly-traded companies to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience.
- The Good: Cybersecurity Predictions 2023 | What's Next?

The Good and the Bad in Cybersecurity: Week 30

The Bad:

- The Bad: Can You Count the Number of Known Vulnerabilities on Your Enterprise?
- The Bad: The Security Incident Response Rules
- The Bad: Ivanti Endpoint Manager patch for mobile devices is vulnerable to a zero-day attack

The Good:

- The Good: The SEC proposes new rules that will require publicly-traded companies to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and experience.
- The Good: Cybersecurity Predictions 2023 | What's Next?