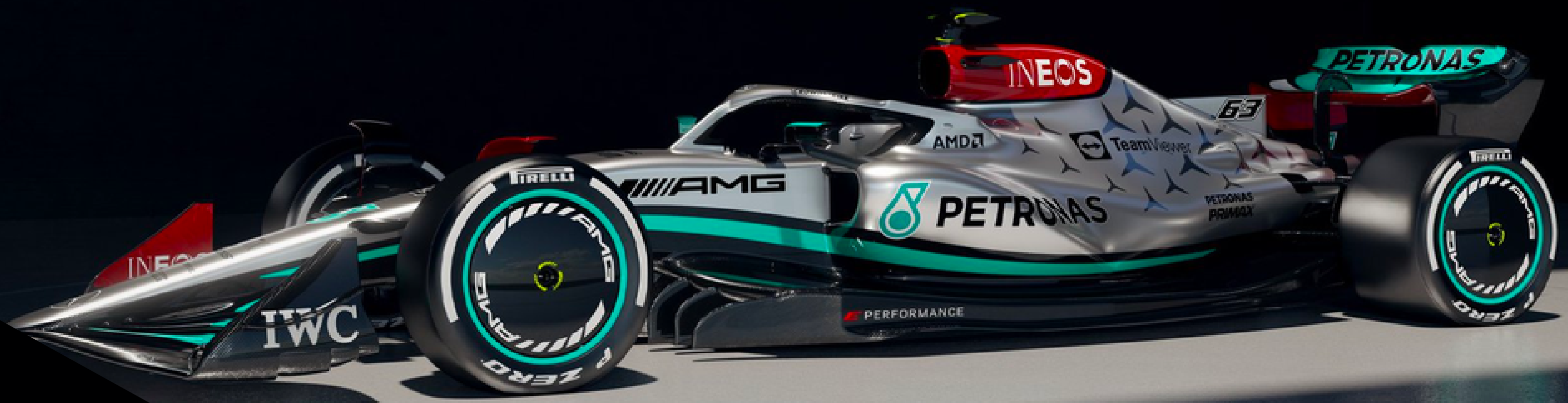


SECURITY PATCHING POLICY

MERCEDES AMG PETRONAS F1 TEAM

Corporate & Automotive Racing Technology

SCOPE

This document aims to outline the organization's procedures for testing, verifying, deploying, and monitoring all technology in accordance with industry best practices. Patching is highlighted as a crucial aspect of vulnerability management, significantly reducing technology susceptibility to risks. Common patching mistakes, such as disconnects between Information Technology (IT) and Cybersecurity teams, unclear priorities, and informal policies, are addressed to ensure clarity and alignment in our approach.

OUR TECHNOLOGY

Mercedes AMG Petronas Formula One Team (MAPFT) operates two distinct technology systems: one for corporate functions and another for automotive racing. This document outlines protocols for patching both technology types, ensuring comprehensive vulnerability management from end to end.

STRATEGY

MAPFT's patching strategy aligns with industry best practices and adheres to vendor recommendations for planning, strategy, technical configurations, and lifecycle management. Our approach is guided by the standards outlined in the National Institute of Standards and Technology (NIST) Guide for Enterprise Management Planning.

The MAPFT patching phases encompass acquiring the patch, testing, deployment, verification, and monitoring.

1. Acquire
During the patch acquisition phase, our team promptly acquires patches released by vendors, with the majority obtained directly from them, while a select few are internally scripted.

2. Test
Subsequently, patches undergo rigorous testing on a small beta group of users or machines to ensure a seamless transition to the upgraded version.

3. Deploy
Once a patch is confirmed to be effective and free of issues, it undergoes deployment across all relevant technology within the organization. In the event there is an issue with a patch most of our assets have rollback procedures available.

4. Verify & Monitor
The deployment process is followed by thorough verification within the CrowdStrike system to ensure that patches are successfully installed and is continuously monitored. This ensures ongoing patch effectiveness and security compliance.

WHY PATCHING

Patching is crucial for workplace and racing technology, ensuring security, stability, and performance. In the workplace, it mitigates vulnerabilities, protects data, and bolsters cybersecurity. Similarly, in racing, patching maintains system reliability, safety, and peak performance, minimizing downtime and enhancing competitiveness. Overall, patching safeguards technology by promoting efficiency and trust.

TYPES OF PATCHING

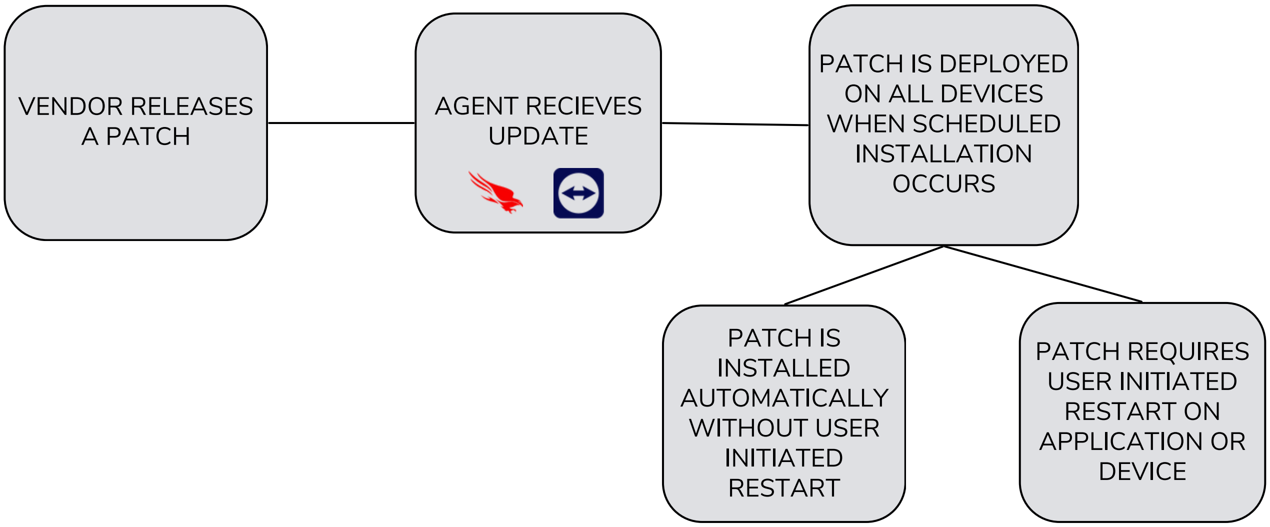
Patching within MAPFT encompasses various types tailored to different technologies and vendors. Third-party patching utilizes vendor-specific tools for applications and web browsers, while operating system patching updates the software running on computers and devices. Network patching applies updates to network devices like routers and firewalls, enhancing network security. Firmware patching involves updating embedded software in hardware devices such as routers and printers, ensuring their stability and functionality. Hardware patching, vital for maintaining the integrity of the organization's IT infrastructure, addresses vulnerabilities and enhances performance across hardware components.

STRATEGY

DEPLOYMENT

Our patch verification, deployment, and monitoring processes are tailored to the capabilities of each application. If an agent lacks certain functionalities, we explore alternative methods for vulnerability management. Currently, our self-updating agents, provided by Crowdstrike and TeamViewer, are installed on all technologies, ensuring seamless remote patching on a scheduled basis.

PATCH LIFE CYCLE


VENDOR RELEASES A PATCH
AGENT RECIEVES UPDATE
PATCH IS DEPLOYED ON ALL DEVICES WHEN SCHEDULED INSTALLATION OCCURS
PATCH IS INSTALLED AUTOMATICALLY WITHOUT USER INITIATED RESTART
PATCH REQUIRES USER INITIATED RESTART ON APPLICATION OR DEVICE

UNDERSTANDING THE RISKS

Patching poses risks, especially when updates require user-initiated restarts. Addressing such challenges underscores the importance of effective employee training and cybersecurity practices. Emphasizing the benefits of periodic device shutdowns fosters teamwork and ensures seamless implementation.

NAVIGATING RISKS

MPAFT has defined three important risk response scenarios using the NIST Preventative Maintenance for Technology. The examples below encompass the Cybersecurity team and IT approach:

- **Routine Patching**

Standard patching procedures apply to regularly scheduled releases. These patches may disrupt daily operations as users may need to perform user-initiated restarts. However, delays in these routine restarts can compound issues later on and increase the complexity of emergency patching and creating windows of opportunity for attackers. All MAPFT assets are currently scheduled for updates on a biweekly basis during non business hours to avoid operational disruptions.

- **Emergency Patching**

This outlines the process for addressing patching emergencies in crisis situations, such as severe vulnerabilities and active exploits. If vulnerable assets are compromised, emergency patching becomes part of incident response. These patches are also made available due to issues with an already released patch. In a known situation where there is a flawed patch, operational disruption patch, or a compromised patch the team must deliberate on whether applying any of these patches is effective based on various factors in consideration:

  - the inventory of affected systems by the vulnerability
  - the importance of the asset
  - data sensitivity
  - available workarounds
  - vendor recommendations

Patch Type	Definition
Flawed Patch	Does not address the known vulnerability
Operational Disruption	Causes a operational disruption
Compromised Patch	A potentially malicious patch

- **Unpatchable Assets**

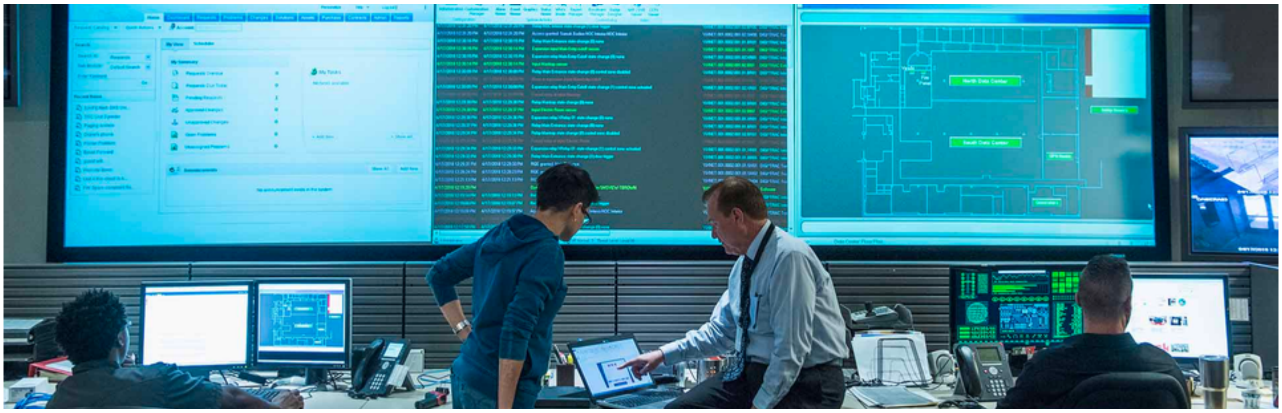
This involves isolating or employing alternative methods to mitigate the risk of systems that are not easily patchable. This is necessary when routine patching cannot be promptly applied, often due to reasons like vendors not providing patches (e.g., end-of-life assets), or the need for uninterrupted operation in mission-critical functions.

MAINTENCE GROUPS

Each asset within our organization is assigned to a maintenance group, facilitating efficient patch grouping based on asset similarity and maintenance requirements. These groups are then allocated specific actions based on predefined risk scenarios. For routine patching, updates are initially deployed on a small subset of users before being rolled out across all systems, with forced installations utilized when grace periods expire. In emergency patching situations, a similar approach is employed, albeit at an accelerated pace depending on the urgency of the vulnerability. Additionally, for assets deemed unpatchable, alternative mitigation methods such as segmentation capabilities are explored, underscoring the multifaceted approach to risk management at MAPFT, where patching represents just one facet among several mitigation strategies.

RISK MANAGEMENT PROCUREMENT

MAPFT incorporates technology maintenance considerations during procurement. Information security and IT managers work closely to establish an evaluation criteria for patching priorities. Vendors are provided with a questionnaire to gather information on updates for vulnerabilities, patch release frequency, vulnerability disclosure, recommendations, support, emergency patching availability, rollback capability, incident response programs, and operational disruptions. These inquiries are crucial as vendor transparency is pivotal in vendor selection.



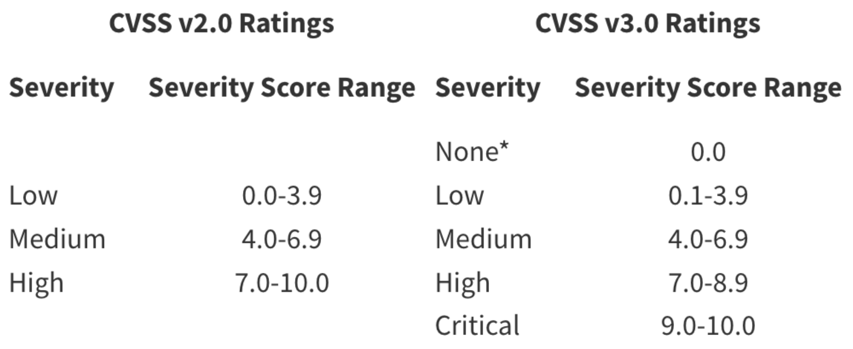
PATCHING BY SEVERITY

SEVERITY STRATEGY

MAPFT utilizes both the Common Vulnerability Scoring System (CVSS) scoring system and an internal asset scoring system to determine the prioritization of patches. When either of the outlined risk scenarios occurs, the risks are escalated to senior management. The Plan of Action (POA) is then decided upon by upper management, comprising C-suite executives and the Chief Information Security Officer (CISO)/Chief Security Officer (CSO).

CVSS SCORING SYSTEM

MAPFT leverages CVSS from NIST National Vulnerability Database as a metric to determine the severity of a vulnerability. The two most common CVSS versions currently used are CVSS v2.0 and CVSS v3.0. The qualitative severity ratings are listed below.



CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

INTERNAL ASSET SCORING SYSTEM

All internal assets utilized at MAPFT undergo scoring on a significance scale, considering factors such as:

- Criticality to business functions
- Sensitivity of data
- Complexity and interdependencies
- Historical vulnerabilities

These assets undergo regular updates and reassessment every quarter in response to the evolving threat landscape.

RACING TECHNOLOGY

OVERVIEW

MAPFT employs various racing technologies, providing a broad overview that includes:

- Telematic Systems
- Engine Control Units (ECUs)
- Engine Recovery Systems (ERS)
- Aerodynamic Control Systems
- Gearbox and Transmission Control Software
- Chassis Control Systems
- Driver Assistance Systems
- Simulation Software

Detailed information about MAPFT asset inventory is available in our internal documentation forums. These forums include specifics such as vendor names, licensing details, access procedures, and additional relevant information.

RACING TECHNOLOGY

UNDERSTANDING OUR TECHNOLOGY

Ensuring the seamless functionality of each integral system and technology is paramount for the team's overall performance. Telematic Systems play a pivotal role by collecting real-time data from sensors during testing and racing, encompassing engine performance, tire conditions, fuel levels, aerodynamics, and critical parameters.

Engine Control Units (ECUs) govern various aspects of the power unit, necessitating software updates for performance optimization, efficiency improvements, and addressing race-identified issues. Engine Recovery Systems (ERS) recover and deploy energy during braking and acceleration, with updates crucial for optimizing energy management, improving reliability, and ensuring race regulation compliance.

Frequent updates are required for Aerodynamic Control Systems due to changing track conditions. Gearbox and Transmission Control Software, Chassis Control Systems, and Driver Assistance Systems, including adaptive steering and brake-by-wire systems, may also require updates for fine-tuning parameters and enhancing driver control. Simulation Software, employed to model and predict car behavior under diverse conditions, benefits from updates to improve accuracy and facilitate the development of optimal race strategies.

VENDOR RELATIONS

MAPFT prioritizes maintaining strong relationships with all our vendors, ensuring that support is readily available for nearly all assets. If necessary, escalation to the vendor is feasible, and their recommendations are valued and considered. Additionally, our remote management software facilitates seamless transitions between updates. With tools like TeamViewer and CrowdStrike, assistance is readily accessible, contributing to efficient and effective patch management processes.

Utilizing CrowdStrike's cloud-native Falcon platform, MAPFT benefits from enhanced visibility, secure system access, and centralized control, regardless of the location of our staff or systems. The Falcon agent facilitates quick searches across our distributed environment, enabling us to identify vulnerable systems promptly. Leveraging Real Time Response our teams can securely access systems remotely for administration tasks, remediation actions, or forensics data collection, without the need for physical access. This is especially important due to the scattered team functions during race events. Admins can run built-in commands and PowerShell scripts, to effortlessly execute tasks, ensuring the ongoing security and integrity of our systems.

Name	Acquire & Validate	Deploy & Verify	Monitor	Restart Required	Rollback Procedure
Telematic Systems	Bosch	CrowdStrike	CrowdStrike	Y	Y
Engine Control Units (ECUs)	Bosch	CrowdStrike	CrowdStrike	Y	Y
Engine Recovery Systems (ERS)	Mercedes High Performance Power Train (HPP)	CrowdStrike	CrowdStrike	Y	Y
Aerodynamic Control Systems	Mercedes High Performance Power Train (HPP)	CrowdStrike	CrowdStrike	Y	Y
Gearbox and Transmission Control Software	Xtrac	CrowdStrike	CrowdStrike	Y	N
Chassis Control Systems	Bosch	CrowdStrike	CrowdStrike	Y	Y
Driver Assistance Systems	Bosch	CrowdStrike	CrowdStrike	Y	Y
Simulation Software	CGTech VERICUT	CrowdStrike	CrowdStrike	Y	Y

OFFICE TECHNOLOGY

OVERVIEW

MAPFT employs various office technologies, providing a broad overview that includes:

- Endpoint Technology
- Documentation Software & Applications
- Project Management Tools
- Communication Systems
- Data Storage & Servers
- 3D Printing & Prototyping
- Modeling Software
- Financial Software
- HR Management Software
- Collaboration Platforms
- Video Analysis Systems
- Training Software
- Office Hardware Supplies
- Security Systems

Detailed information about these assets is available in our internal asset documentation forums. These forums include specifics such as vendor names, licensing details, access procedures, and additional relevant information.

OFFICE TECHNOLOGY

UNDERSTANDING OUR TECHNOLOGY

MAPFT utilizes a diverse array of systems and technologies to maintain a seamless workforce and operational structure. Patching of office technology, including crucial endpoint devices like tablets, personal computers, and cellphones, is prioritized to ensure continuous security and functionality.

Access to corporate apps on personal devices is contingent upon having the latest version installed. Documentation software, such as Microsoft Office applications, fulfills all documentation needs, while project management tools aid in coordinating tasks and tracking timelines. Communication systems, encompassing conferencing apps, messaging, email, and collaboration platforms, undergo regular patching according to established schedules. Data storage and servers manage extensive volumes of racing and performance data, necessitating robust patching protocols.

3D printing and prototyping software, coupled with modeling tools, uphold precision in creating accurate prototypes essential for team operations. Financial and HR management systems contribute to corporate technology functionality, while video analysis tools facilitate race footage review and driver performance analysis. Training simulators offer virtual environments for driver training, simulating real racing conditions. Security systems and hardware, including both physical and virtual security applications, are vital components of our infrastructure, ensuring comprehensive protection.

Name	Acquire & Validate	Deploy & Verify	Monitor	User Initiated Restart Required	Rollback Procedure
Endpoint Technology	HPE	CrowdStrike	CrowdStrike	Y	Y
Documentation Applications	Microsoft	CrowdStrike	CrowdStrike	Y	Y
Project Management Tools	Asana	CrowdStrike	CrowdStrike	Y	Y
Communication Systems	Microsoft	CrowdStrike	CrowdStrike	Y	Y
Data Storage & Servers	HPE	CrowdStrike	CrowdStrike	Y	Y
3D Printing & Prototyping	HPE	CrowdStrike	CrowdStrike	Y	Y
Modeling Software	Siemens	CrowdStrike	CrowdStrike	Y	Y
Financial Software	SAP	CrowdStrike	CrowdStrike	Y	Y

Name	Acquire & Validate	Deploy & Verify	Monitor	User Initiated Restart Required	Rollback Procedure
HR Management	SAP	CrowdStrike	CrowdStrike	Y	Y
Collaboration Platforms	Microsoft	CrowdStrike	CrowdStrike	Y	Y
Video Analysis Systems	VimBiz	CrowdStrike	CrowdStrike	Y	Y
Training Software	SAP	CrowdStrike	CrowdStrike	Y	Y
Office Hardware	HPE, Vodafone	CrowdStrike	CrowdStrike	Y	N
Physical Security Systems	Bosch	CrowdStrike	CrowdStrike	Y	Y
Virtual Security Systems	CrowdStike	CrowdStrike	CrowdStrike	Y	Y

REFERENCES

[1]
M. Souppaya, “Guide to Enterprise Patch Management Planning”:, 2022, doi: https://doi.org/10.6028/nist.sp.800-40r4.

[2]
“FIA issues tender for standard F1 gearbox supplier from 2021 season,” www.autosport.com, Feb. 19, 2019. https://www.autosport.com/f1/news/fia-issues-tender-for-standard-f1-gearbox-supplier-from-2021-season-5283995/5283995/ (accessed Feb. 15, 2024).

[3]
“Patch Management,” TeamViewer. https://www.teamviewer.com/en-us/products/remote/solutions/patch-management/

[4]
CrowdStrike, “Patch Management: What It Is & Best Practices | CrowdStrike,” crowdstrike.com, Feb. 28, 2022. https://www.crowdstrike.com/cybersecurity-101/patch-management/

[5]
R. Scobey, “Vulnerability Patching for a Remote Workforce,” crowdstrike.com, Apr. 17, 2020. https://www.crowdstrike.com/blog/tech-center/patching-remote-workforce/ (accessed Feb. 15, 2024).

[6]
“MERCEDES-AMG PETRONAS FORMULA ONE - VERICUT USA,” cgtech.com. https://cgtech.com/component/k2/item/456-mercedes.html#:~:text=The%20machine%20shop%20of%20the (accessed Feb. 15, 2024).

APPENDIX

Selected acronyms and abbreviations used in this document are shown below.

CISO	Chief Information Security Officer
CSO	Chief Security Officer
CVSS	Common Vulnerability Scoring System
ECU	Engine Control Unit
ERS	Engine Recovery System
HPE	Hewlett Packard Enterprise
IT	Information Technology
MAPFT	Mercedes AMG Petronas Formula One Team
NIST	National Institute of Standards and Technology
POA	Plan of Action